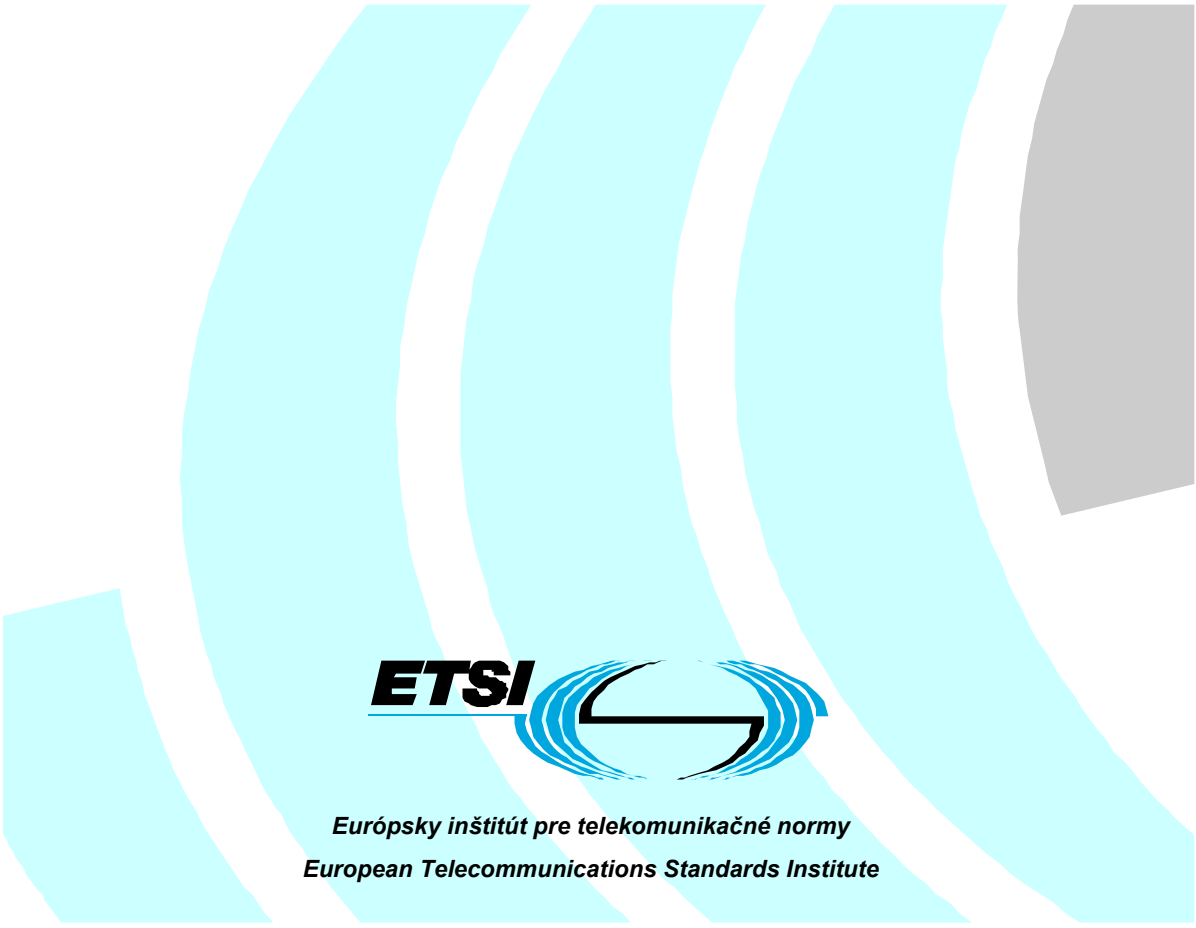
ETSI TS 102 367 V1.2.1 (2006-01)

Technická špecifikácia

Digitálne rozhlasové vysielanie (DAB); Podmienený prístup

Digital Audio Broadcasting (DAB);
Conditional access



Európsky inštitút pre telekomunikačné normy

European Telecommunications Standards Institute

Referenčné číslo

RTS/JTC-DAB-46

Deskriptory

audio, broadcasting, DAB, data, digital

ETSI

650 Route des Lucioles

F–06921 Sophia Antipolis Cedex – France

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C

Neziskové združenie registrované
na podprefektúre de Grasse (06) N° 7803/88

Dôležité upozornenie

Jednotlivé kópie tohto dokumentu možno stiahnuť zo stránky:

http://pda.etsi.org

Tento dokument môže byť dostupný vo viacerých elektronických verziách alebo v tlačenej forme. V prípade existujúceho alebo viditeľného rozdielu v obsahu medzi takýmito verziami je referenčnou verziou verzia v prenosnom dokumentovom formáte (Portable Document Format – PDF).

V prípade sporu je referenčným výtlačok vytlačený na tlačiarni ETSI z verzie PDF uchovávanej na určenom sieťovom serveri sekretariátu ETSI.

Používatelia tohto dokumentu by mali brať do úvahy, že dokument môže byť revidovaný alebo sa môže zmeniť jeho postavenie. Informácie o postavení tohto dokumentu a ďalších dokumentov ETSI sú dostupné na http://portal.etsi.org/tb/status/status.asp

Ak nájdete v tomto dokumente chyby, svoje pripomienky zašlite na:

http://portal.etsi.org/chaircor/ETSI_support.asp

Oznam o autorských právach

Obsah

Práva duševného vlastníctva

Práva duševného vlastníctva, ktoré majú alebo môžu mať zásadný význam pre tento dokument, mohli byť oznámené organizácii ETSI. Informácie o týchto zásadných právach duševného vlastníctva, ak existujú, sú pre členov i nečlenov ETSI verejne dostupné a môžu ich nájsť v dokumente ETSI SR 000 314 s názvom Práva duševného vlastníctva (IPR), ktorý možno získať na sekretariáte ETSI. Najnovšie znenie je dostupné na serveri ETSI (http://webapp.etsi.org/IPR/home.asp).

V súlade so svojou politikou v oblasti práv duševného vlastníctva ETSI nevyhľadáva ani neskúma nijaké práva duševného vlastníctva. Neposkytuje ani záruku týkajúcu sa existencie iných IPR, ktoré nie sú uvedené v dokumente ETSI SR 000 314 (alebo v jeho aktualizovaných vydaniach na serveri ETSI), ktoré majú, môžu mať, alebo môžu nadobudnúť zásadný význam pre predkladaný dokument.

Predhovor

Technickú špecifikáciu (TS) vytvorila spojená technická komisia (JTC) Vysielanie Európskej vysielacej únie (EBU), Európskeho výboru pre normalizáciu v elektrotechnike (CENELEC) a Európskeho inštitútu pre telekomunikačné normy (ETSI).

POZNÁMKA. – JTC EBU/ETSI na vysielanie bola zriadená v roku 1990 s cieľom koordinovať návrhy noriem pre danú oblasť vysielania a v priradených oblastiach. Od roku 1995 sa JTC na vysielanie stala trojstranným orgánom, keď do Memoranda o porozumení bol zahrnutý i CENELEC, ktorý je zodpovedný za normalizáciu rozhlasových a televíznych prijímačov. EBU je profesionálnym združením vysielacích organizácií, ktorých práca zahŕňa koordináciu aktivít jej členov v technickej a legislatívnej oblasti a v oblasti výroby a výmeny programov. EBU má aktívnych členov asi v 60 krajinách európskej vysielacej oblasti; jej sídlo je v Ženeve.

European Broadcasting Union
CH-1218 GRAND SACONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

Projekt Eureka 147 bol založený v roku 1987, financovaný Európskou komisiou, s cieľom vyvinúť systém na vysielanie rozhlasu a dát na pevný, prenosný a mobilný príjem. Práca projektu je zdokumentovaná v publikácii európskej normy, EN 300 401 [1] DAB (pozri poznámku 2), ktorá má dnes celosvetové uznanie. Členovia projektu Eureka 147 pozostávajú z organizácií vysielateľov, telekomunikačných operátorov spolu so spoločnosťami z profesionálnej oblasti a elektronického priemyslu.

V roku 1995 bolo ustanovené Európske fórum DAB (EuroDAB) na sledovanie zavádzania služieb DAB konkrétnym spôsobom po celom svete a v roku 1997 sa stalo z neho Svetové fórum DAB (World DAB).

POZNÁMKA 2. – DAB je registrovaná značka, ktorú vlastní jeden z partnerov projektu EUREKA 147.

1 Predmet

Systémy podmieneného prístupu poskytujú DAB schopnosť distribuovať zvukové aj dátové zakódované služby. Táto technická špecifikácia špecifikuje normalizovaný rámec, ktorý definuje, ako sa prenášajú zakódované služby v systéme digitálneho rozhlasového vysielania. Rámec je otvorený integrácii rozličných systémov podmieneného prístupu, ako aj integrácii systémov so skramblerom.

2 Referenčné dokumenty

Tieto dokumenty obsahujú ustanovenia, ktoré prostredníctvom odkazov v texte tvoria ustanovenia tejto technickej špecifikácie.

- Odkazy sú špecifikované (určené dátumom vydania, číslom vydania, číslom verzie atď.) alebo nešpecifikované.
- V prípade špecifikovaného odkazu neplatia ďalšie revízie.
- V prípade nešpecifikovaného odkazu platí posledná verzia.

Referenčné dokumenty, ktoré sú verejne nedostupné na bežnom mieste, možno nájsť na http://docbox.etsi.org/Reference.

[1] ETSI EN 300 401: Radio Broadcasting Systems – Digital Audio Broadcasting (DAB) to mobile, portable and fixed receivers

2] EN 301 234: Digital Audio Broadcasting (DAB) – Multimedia Object Transfer (MOT) protocol.

3 Termíny, definície, skratky a dohody

3.1 Termíny a definície

V dokumente sa používajú definície uvedené v EN 300 401 [1] a termíny a definície:

podmienený prístup CA (angl. **Conditional Access CA):** mechanizmus, ktorým sa môže obmedziť prístup používateľa k zložkám služby

riadiace slovo CW (angl. **control word CW):** kľúč alebo časť kľúča, ktoré sa používajú na šifrovanie alebo dešifrovanie obsahu

dátové pole predvoľby (angl. **prefix data field):** telo predvoľby podmieneného prístupu subkanála

záhlavie predvoľby (angl. **prefix header):** záhlavie predvoľby podmieneného prístupu subkanála

systém so skramblerom SSS (angl. **shared scrambler system SSS):** systém poskytujúci synchronizáciu rôznych systémov CA, kde jednu službu poskytujú viacerí poskytovatelia CA so súčasným skramblovaním obsahu

POZNÁMKA. – Okrem modulu systémového dekódovača CA prijímače obsahujú deskrambler.

3.2 Skratky

V dokumente sa používajú skratky definované v normách EN 300 401 [1] a EN 301 234 [2] a skratky:

BWS	Broadcast WebSite	webová stránka vysielania
CA	Conditional Access	podmienený prístup
CACC	Conditional Access Communication Controller	riadiaca jednotka komunikácie podmieneného prístupu
CAFlag	Conditional Access Flag	návesť podmieneného prístupu
CAId	Conditional Access Identifier	identifikátor podmieneného prístupu
CAIndi	Conditional Access Indicator field	pole indikátora podmieneného prístupu
CAIntChar	Conditional Access system Internal Characteristics	podmienený prístup k systému vnútorných charakteristík
CAIntMess	Conditional Access system Internal Messages	podmienený prístup k systému vnútorných správ
CAIntMess Field	Conditional Access system Internal Messages Field	pole podmieneného prístupu k systému vnútorných správ
CAMode	Conditional Access Mode	mód podmieneného prístupu
CAOrg	Conditional Access Organization	usporiadanie podmieneného prístupu
CAOrgFlag	Conditional Access Organization Flag	návesť usporiadania podmieneného prístupu
CAOrgIndi	Conditional Access Organization Indicator field	pole indikátora usporiadania podmieneného prístupu
CASyncPa ram	Conditional Access Synchronization Parameters	synchronizačné parametre podmieneného prístupu
CASysId	Conditional Access System Identifier	identifikátor systému podmieneného prístupu
CASysIdLi st	List of Conditional Access System Identifiers	zoznam identifikátorov systému podmieneného prístupu
Ch	Channel	kanál
CW	Control Word	riadiace slovo
CWT	Control Word Toggle bit	prepínací bit riadiaceho slova
DGCAPrefi x	Data Group Conditional Access Prefix	predvoľba skupiny dát podmieneného prístupu
EEP	Equal Error Protection	zabezpečenie proti rovnakým chybám
FIDC	Fast Information Data Channel	rýchly kanál dátových informácií
GSM	Global System for Mobile communication	globálny systém mobilných komunikácií
IP Tunnel	Internet Protocol Tunnelling	výstavba kanála s internetovým protokolom
LSb	Least Significant bit	bit s najmenším významom
MOT DirMod	MOT Directory Mode	mód zoznamu MOT
MOT HdMode	MOT Header Mode	mód záhlavia MOT
MOTCAPr efix	MOT Conditional Access Prefix	predvoľba podmieneného prístupu MOT
MPEG2-TS	MPEG2 Transportation Stream	transportný tok MPEG2
MSb	Most Significant bit	najvýznamnejší bit
MSC	Main Service Channel	kanál hlavnej služby
PAD	Programme Associated Data	dáta priradené k programu

SharedFlag	Shared scrambler Flag field	spoločná návesť poľa so skramblerom
ShortCASysId	Short Conditional Access System Identifier	krátky identifikátor systému podmieneného prístupu
SLS	SLide Show	prezentácia
SSS	Shared Scrambler System	systém so skramblerom
SUBCAPrefix	SUB-channel Conditional Access Prefix	predvoľba podmieneného prístupu subkanála
TDC	Transparent Data Channel	transparentný dátový kanál

3.3 Dohody

Čo sa týka poradia bitov, v každom kroku spracovania, ak nie je ustanovené inak, používa sa tento spôsob zapisovania:

– bit umiestnený v obrázkoch v ľavej pozícii sa považuje za prvý;

– bit umiestnený v tabuľkách v ľavej pozícii sa považuje za prvý;

– v bajtových poliach sa najvýznamnejší bit (msb) považuje za prvý a označuje sa najvyšším číslom; napríklad msb jedného bajtu je označený b7 a bit s najmenším významom (lsb) je označený b0;

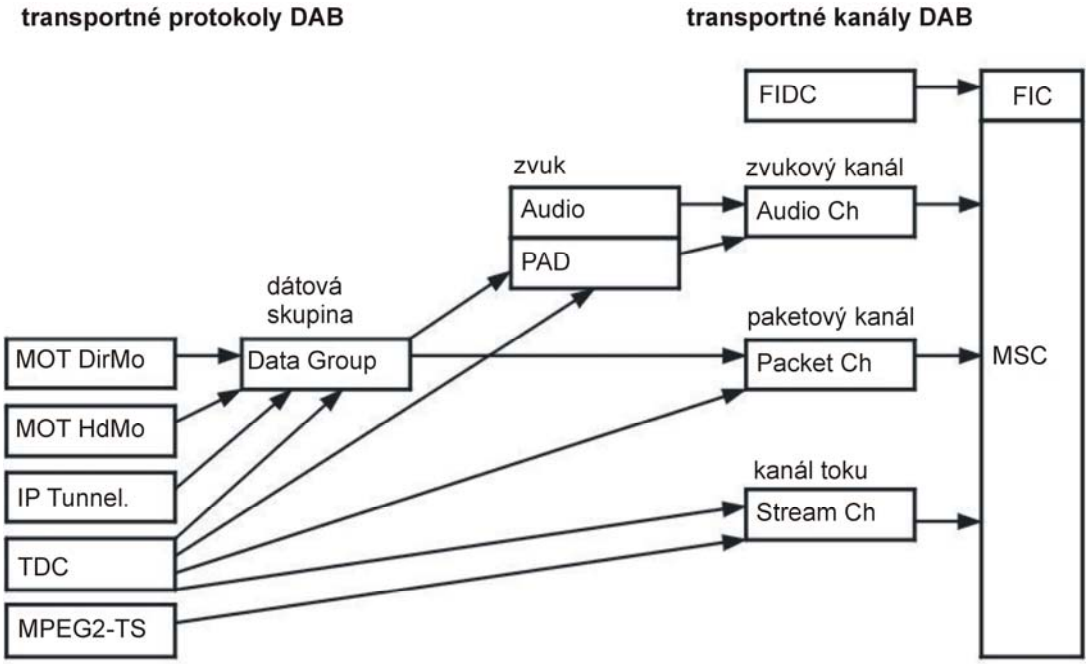
– vo vektoroch (matematických výrazoch) sa prvok s najnižším indexom považuje za prvý.

POZNÁMKA. – Z dôvodu časového prekladania toto poradie bitov nie je skutočným prenosovým poradím. Čierny trojuholník v obrázkoch znamená, že príslušný prvok je skramblovaný.

4 Úvod

4.1 Všeobecný opis

Táto časť špecifikácie znázorňuje prehľad existujúcich transportných protokolov DAB a transportných kanálov DAB.



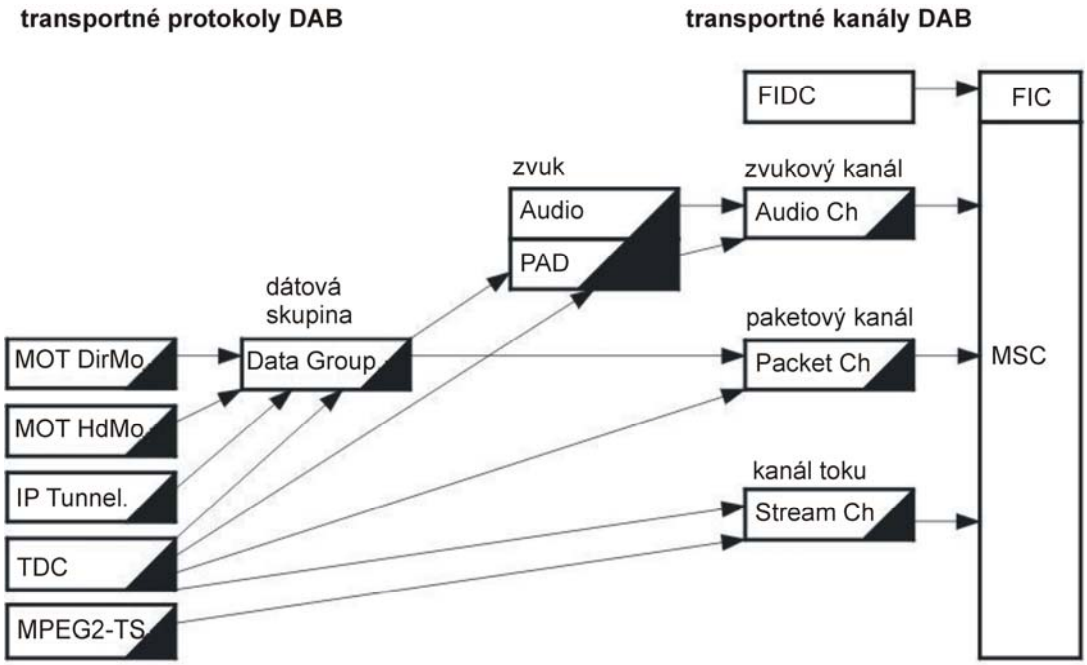
Obrázok 1 – Prehľad transportných protokolov DAB a transportných kanálov DAB

4.2 Módy skramblovania

Systémy podmieneného prístupu sa môžu aplikovať na rôznych úrovniach. Táto časť špecifikácie opisuje tri transportné úrovne DAB vhodné na podmienený prístup a ilustruje vplyv na vyššie transportné úrovne, ktoré sú v obrázkoch 2, 3 a 4 označené čiernymi trojuholníkmi.

4.2.1 Subkanály skramblovania DAB

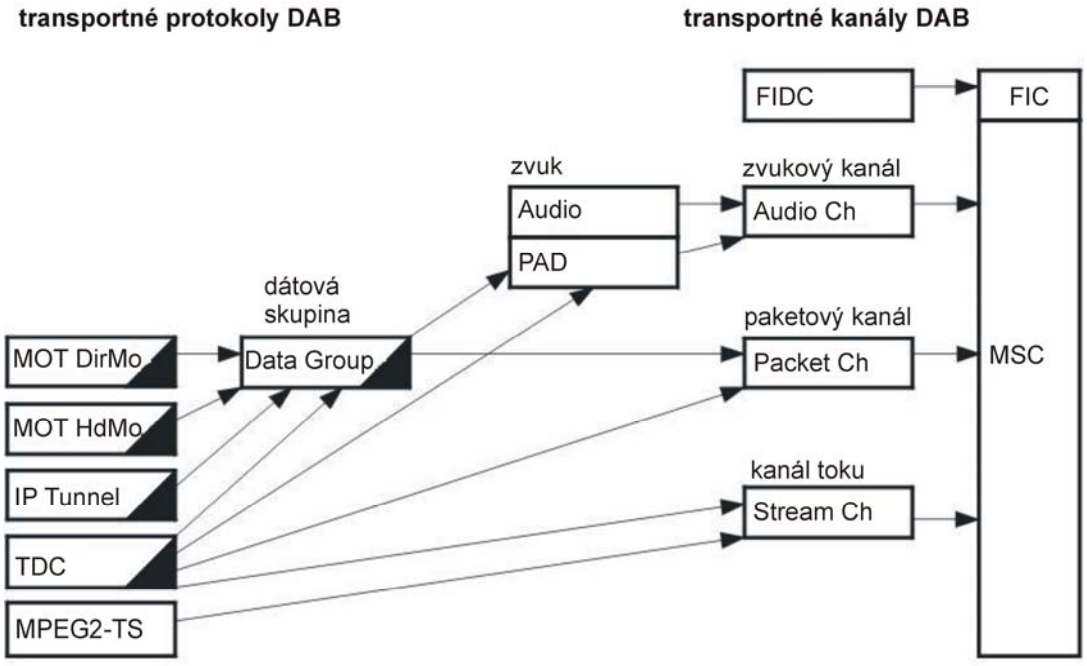
Subkanál CA: Šifruje kompletný subkanál, napríklad rozhlasový subkanál vrátane PAD alebo úplný subkanál v móde paketov, alebo subkanál v móde toku.



Obrázok 2 – Aplikácia a vplyv subkanála CA

4.2.2 Skramblovanie dátových skupín DAB

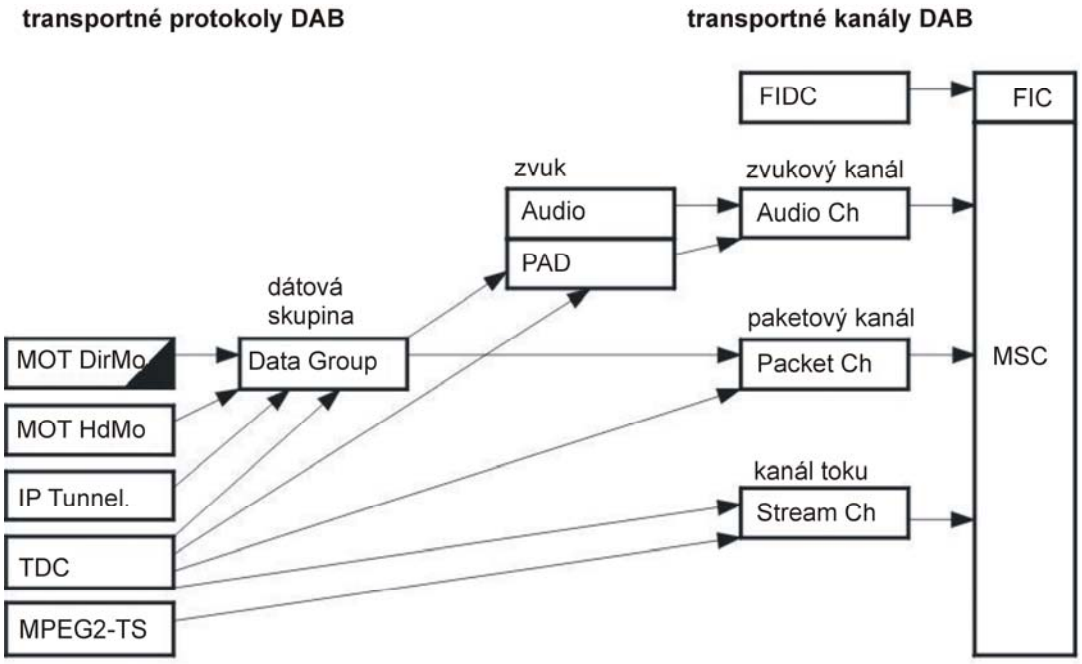
Dátová skupina CA: Umožňuje šifrovanie všetkých dát prenosových protokolov DAB, ktoré používajú dátové skupiny MSC, ako výstavba kanála IP, MOT, TDC atď.



Obrázok 3 – Aplikácia a vplyv dátovej skupiny CA

4.2.3 Skramblovanie objektov MOT

MOT CA: Umožňuje šifrovanie súborov aktualizovaných použitím módu zoznamu MOT, napríklad vybraných častí webovej stránky vysielania (BWS).



Obrázok 4 – Aplikácia a vplyv MOT CA

4.3 Koncepcia systému podmieneného prístupu

Prvky systému podmieneného prístupu možno rozdeliť na systémové prvky CA vysielacej strany a systémové prvky CA prijímacej strany.

Systémové prvky CA na vysielacej strane: kódovač poľa podmieneného prístupu k systému vnútorných správ, generátor riadiaceho slova, synchronizátor a skrambler.

Na vstupe týchto prvkov sa poskytujú účastnícke dáta, dáta poskytovateľa CA a neskramblovaný obsah.

– **Kódovač poľa podmieneného prístupu k systému vnútorných správ:** Generuje správy, napríklad riadiace správy týkajúce sa oprávnení používateľa, alebo správy, ktoré obsahujú aktuálne riadiace slovo a aktivujú kontrolu oprávnenia na prijímacej strane. Tieto správy a formáty správ sú špecifické danému systému CA a jednotlivé systémy CA sa vzájomne odlišujú. V ďalšom texte je CAIntMess nazvané pole podmieneného prístupu k systému vnútorných správ a nie je podrobne opisované. Polia podmieneného prístupu k systému vnútorných správ sa môžu prenášať v multiplexe.

  POZNÁMKA. – V hybridných systémoch sa môžu polia podmieneného prístupu k systému vnútorných správ prenášať v iných kanáloch, napríklad v GSM.

– **Generátor riadiaceho slova:** Poskytuje riadiace slová, ktoré potrebuje skrambler, ako aj kódovač poľa podmieneného prístupu k systému vnútorných správ a poskytuje ich synchronizátoru.

– **Synchronizátor:** Synchronizuje proces skramblovania a dispečingu riadiaceho slova a podáva riadiace slovo prvkom skramblera a kódovača poľa CA a okrem toho generuje parametre synchronizácie CA (CASyncParam), ktoré umožňujú prijímaču synchrónne dekódovať správy a deskramblovať obsah. Synchronizačné parametre CA tvoria súčasť multiplexu.

– **Skrambler:** Skrambluje prichádzajúci obsah príslušným riadiacim slovom.

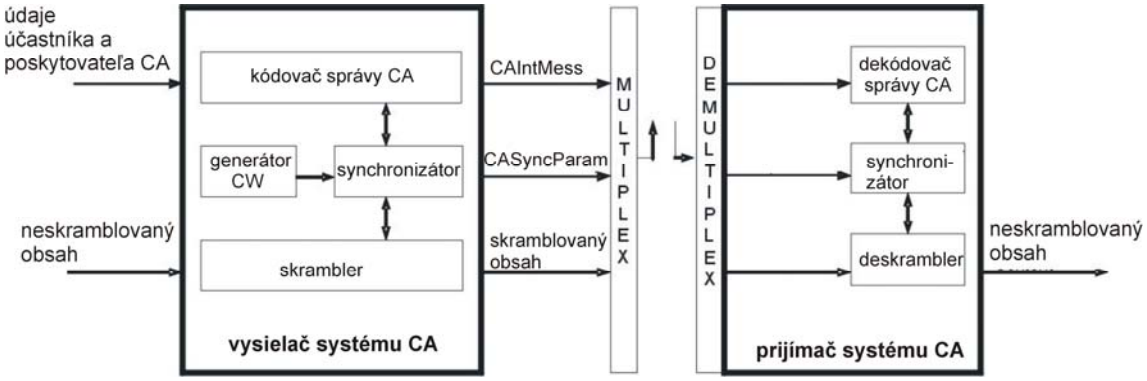
  Skramblovaný obsah tvorí súčasť multiplexu.

Systémové prvky CA na prijímacej strane: dekódovač poľa CA, synchronizátor, deskrambler.

– **Dekódovač poľa CA:** Interpretuje polia podmieneného prístupu k systému vnútorných správ a štartuje zodpovedajúce procedúry manažérstva oprávnenia, kontroly oprávnenia a spracovania riadiaceho slova.

– **Synchronizátor:** Intrerpretuje synchronizačné parametre CA a synchrónne posúva riadiace slovo k deskrambleru.

– **Deskrambler:** Deskrambluje skramblovaný obsah pomocou riadiaceho slova.



Obrázok 5 – Koncepcia systému podmieneného prístupu

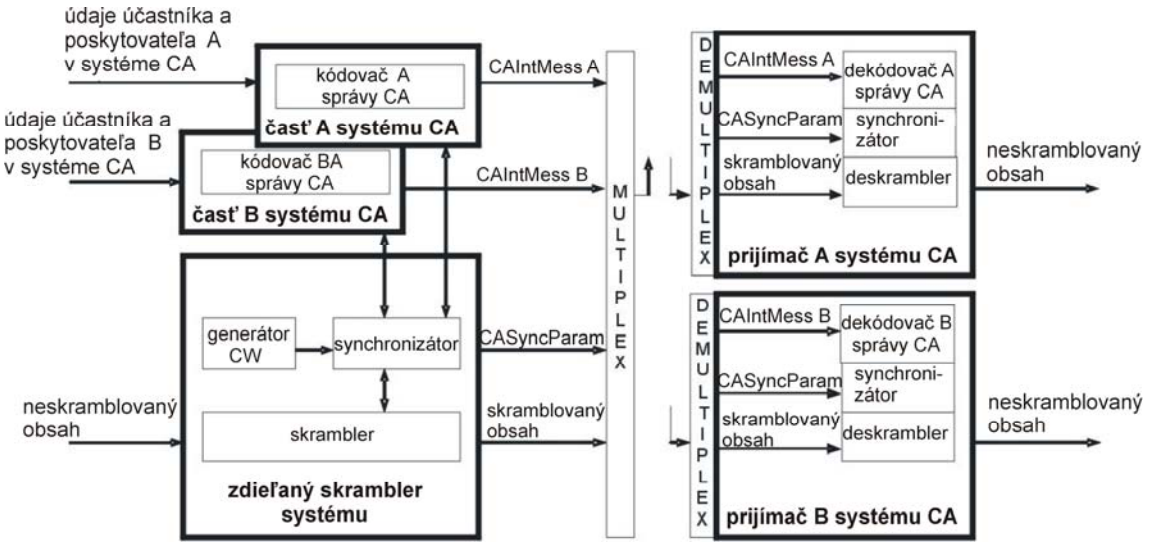
4.4 Koncepcia systému so skramblerom (SSS)

Kde je viac ako jeden poskytovateľ CA na tú istú službu, je vhodné obsah prenášať iba raz, ale súčasne aplikovať rozličné systémy CA.

Z toho dôvodu poskytovatelia CA môžu spolupracovať a skramblovať obsah použitím zdieľaného skramblera. Každý systém CA musí generovať svoje vlastné polia podmieneného prístupu k systému vnútorných správ (CAIntMess), ktoré sa musia synchronizovať so skramblovacím procesom. Koncové zariadenie je schopné interpretovať svoje vlastné polia podmieneného prístupu k systému vnútorných správ, ale má integrovaný modul s deskramblerom na deskramblovanie obsahu.

Návrh systému s integrovaným skramblerom je mimo rozsahu tejto špecifikácie. Koncepty sú otvorené a umožňujú pridanie existujúceho systému s integrovaným skramblerom na vysielacej strane.

POZNÁMKA. – Systém s integrovaným skramblerom sa môže aplikovať vtedy, keď je plánovaná aktualizácia systému CA a obe verzie, stará aj nová, môžu fungovať paralelne počas určitého časového obdobia.



Obrázok 6 – Koncepcia systému s integrovaným skramblerom

Koncepcia systému s integrovaným skramblerom vyžaduje na každú CAIntMess indikátor na rozlíšenie, ku ktorému systému CA patrí. To sa robí prostredníctvom krátkeho identifikátora systému podmieneného prístupu (ShortCASysId). Koncepcia zdieľaného skramblera vyžaduje na skramblovaný obsah indikátor na určenie všetkých systémov CA, ktoré sa podieľajú na skramblovaní. To zabezpečuje pole návesti zdieľaného skramblera (SharedFlag).

5 Parametre: formát, kódovanie a umiestnenie

Je špecifikovaných niekoľko parametrov, ktoré signalizujú prijímaču, či sú dáta skramblované alebo nie, ktorý systém CA a ktorý mód CA sa používa, kde sa nachádzajú polia podmieneného prístupu k systému vnútorných správ a prídavné polia podmieneného prístupu k systému vnútorných charakteristík a ako sa má zadefinovať synchronizovaný deskrambler. Tieto parametre sa špecifikujú ďalej.

5.1 Identifikátor CA (CAId)

Identifikátor CA (CAId) sa signalizuje použitím FIG 0/2 (pozri čl. 6.3.1 EN 300 401 [1]).

Toto trojbitové pole indikuje, či sa používa systém podmieneného prístupu niektorých zo zložiek služby.
Interpretácia tohto poľa:

000: nijaké riadenie prístupu akejkoľvek zložky služby;
001: rezerva;
010: rezerva;
011: rezerva;
100: rezerva;
101: rezerva;
110: rezerva;
111: najmenej jedna zložka služby je skramblovaná; skramblované zložky sa signalizujú podľa tejto špecifikácie.

POZNÁMKA. – Pole CAId môže použiť prijímač na určenie verzie tejto špecifikácie, ktorú použil poskytovateľ služby. Hodnota 111 indikuje prijímaču, že sa použila aktuálna verzia tejto špecifikácie. Hodnoty 001 a 010 indikujú, že na túto špecifikáciu sa použila verzia V1.1.1.

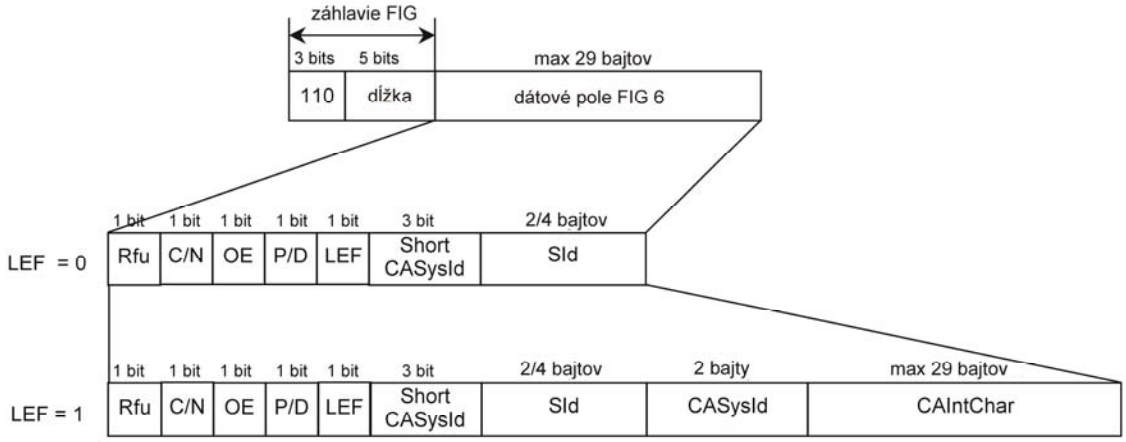
5.2 Zoznam identifikátorov systému CA (CASysIdList)

Zoznam identifikátorov systému podmieneného prístupu CA (CASysIdList) opisuje použitý systém; obsahuje identifikátory a prídavné charakteristiky aktuálne použitého systému CA.

Každý prvok zoznamu CASysIdList sa prenáša v jednom dátovom poli typu FIG 6. Preto dĺžka jedného prvku zoznamu nemá presiahnuť 29 bajtov. Maximálna dĺžka poľa CAIntChar sa teda definuje touto hodnotou. Dĺžka je indikovaná v záhlaví FIG (pozri čl. 5.2.2 EN 300 401 [1]).

Parametre prenášané v zozname CASysIdList sú statickej povahy.

Každý prvok zoznamu CASysIdList obsahuje identifikátor a charakteristiky jedného aktuálne použitého systému CA. Formát je zobrazený na obrázku 7.



Obrázok 7 – Štruktúra dátového poľa FIG typu 6

Používajú sa tieto definície:

Reserved for future use Rfu (rezerva na budúce použitie): Jednobitové pole sa rezervuje na budúce použitie zvyšku štruktúry; aktuálne špecifikovaná definícia – bit Rfu nastavený na nulu.

Current/Next C/N (aktuálny/nasledujúci): Jednobitové pole indikuje verziu informácie o službe (SIV), pozri čl. 5.2.2.1 EN 300 401 [1], situáciu (b).

Other Ensembles OE (ďalšie množiny): Jednobitová návesť indikuje, či sa informácia vzťahuje na túto množinu alebo na inú, pozri čl. 5.2.2.1 EN 300 401 [1].

P/D: Jednobitová návesť indikuje, či sa pole identifikátora služby (Sid) používa na programové služby alebo na dátové služby, pozri čl. 5.2.2.1 EN 300 401 [1].

List Element Flag LEF (návesť zoznamu prvkov): Jednobitová návesť indikuje, či sa signalizuje zmena databázy (CEI) alebo sa prezentuje nejaký prvok zoznamu CASysIdList, a definuje sa týmto spôsobom:

0: zmena databázy, ShortCASysId je nastavený na 000;

1: prezentovaný prvok zoznamu CASysIdList.

ShortCASysId: Trojbitové pole obsahuje krátky identifikátor systému CA, pozri čl. 5.2.2.

Service Identifier SId (identifikátor služby): Dvojbitové alebo štvorbitové pole identifikuje službu; jeho dĺžku signalizuje návesť P/D.

CASysId: Dvojbitové pole identifikuje systém CA, pozri čl. 5.2.1.

CAIntChar: Pole s maximálnou dĺžkou 24 bajtov obsahuje CA k systému vnútorných charakteristík, pozri čl. 5.2.3.

Tento znak používa signalizáciu SIV (pozri čl. 5.2.2.1 EN 300 401 [1]. Databáza je delená použitím databázového kľúča. Zmeny databázy sa signalizujú použitím CEI.

Databázový kľúč obsahuje návesti **OE** a **P/D** a pole **SId**.

Indikácia zmeny udalosti sa signalizuje návesťou prvok zoznamu (**LEF**) = 0.

5.2.1 Identifikátor systému CA (CASysId)

Každý systém CA sa identifikuje prostredníctvom identifikátora systému CA (CASysId).

Formát a kódovanie: Dĺžka je 2 bity. Zoznam aktuálne registrovaných identifikátorov systému CA sa uvádza v prílohe F.

Umiestnenie: Identifikátor každého systému CA aktuálne použitého v multiplexe sa prenáša v zozname prvkov zoznamu identifikátorov systému CA (CASysIdList).

5.2.2 Krátky identifikátor systému CA (ShortCASysId)

Identifikátory systému CA (CASysId) aktuálne použitých systémov CA a ich parametre sa pri vnútornom spracovaní mapujú do dočasného krátkeho identifikátora systému CA (ShortCASysId). Tie sa potom použijú na indikáciu systému CA, ku ktorému každá CAIntMess patrí v prípade aplikácie systému so zdieľaným skramblerom (SSS).

ShortCASysId je jedinečný a platný v rámci jednej služby. Pri jednotlivých komponentoch služby sa môže aplikovaný systém CA odlišovať.

> POZNÁMKA. – Skramblovaný komponent je sprevádzaný poľom návesti (SharedFlag), ktoré identifikuje aplikovaný systém (aplikované systémy) CA (pozri čl. 5.4.2).

Ak viaceré služby používajú spoločný komponent služby, potom mapovanie identifikátora CASysId do ShortCASysID je rovnaké vo všetkých týchto službách a do všetkých ShortCASysIds sa má použiť v spoločnom komponente služby.

Formát a kódovanie: Dĺžka je 3 bity, pričom sa môže špecifikovať až 8 rôznych systémov CA v rámci jednej služby.

Umiestnenie: Krátky identifikátor systému CA, ShortCASysId, každého aktuálne použitého systému CA v multiplexe sa prenáša v zozname prvkov zoznamu identifikátorov systému CA, CASysIdList.

Na priradenie nejakých polí CAIntMess k určitému systému CA sa krátky identifikátor systému CA, ShortCASysId, uvádza v prvých bitoch poľa CAIntMess.

5.2.3 Podmienený prístup k systému vnútorných charakteristík (CAIntChar)

Podmienený prístup k systému vnútorných charakteristík (CAIntChar) je opísaný informáciami, ako je napríklad verzia, aplikovaný algoritmus, špecifické systémové parametre, identifikátor kanála, dĺžka identifikátora, parametre týkajúce sa obsahu, statické predčíslia a podobne.

Formát a kódovanie: Maximálna dĺžka je 24 bitov. Usporiadanie tohto poľa je charakteristické s príslušným systémom CA a v tejto technickej špecifikácii nie je normalizované.

Umiestnenie: Podmienený prístup k systému vnútorných charakteristík každého aktuálne použitého systému CA v multiplexe sa prenášajú v zozname prvkov zoznamu identifikátorov sytému CA (CASysIdList).

5.3 Indikácia CA (CAFlag/CAIndi)

Skramblovaný obsah alebo iný obsah súvisiaci s CA sa indikuje nastavením návesti CA (CAFlag) alebo implicitne existenciou poľa indikátora CA (CAIndi). Indikácia CA je určená hlavne do koncových zariadení bez možnosti CA, čo sa interpretuje týmto spôsobom:

Formát a kódovanie:

– CA nie je indikované – CAFlag nie je nastavený alebo CAIndi nie je prezentované:

– časť obsahu alebo celý obsah je neskramblovaný;

– časť obsahu sa môže skramblovať;

– koncové zariadenia bez možnosti CA má zmysel spracúvať neskramblované časti obsahu;

– koncové zariadenia s možnosťou CA budú spracúvať obsah v každom prípade (skramblované aj neskramblované časti obsahu).

– CA je indikované – Návesť CAFlag je nastavená alebo pole CAIndi sa prezentuje:

– zodpovedajúci obsah je úplne skramblovaný;

– koncové zariadenia bez možnosti CA obsah nespracujú;

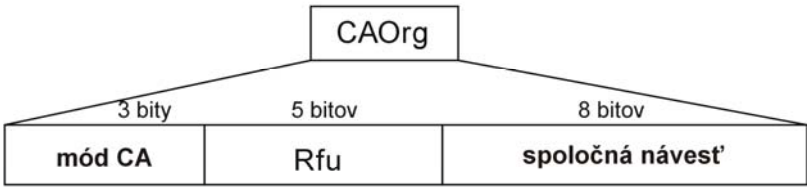
– koncové zariadenia s možnosťou CA obsah spracujú.

Umiestnenie: CA je indikovaný na rozličných úrovniach. Umiestnenie sa detailne uvádza v príslušných článkoch.

5.4 Usporiadanie CA (CAOrg)

Usporiadanie CA obsahuje všeobecnú informáciu o aplikovanom CA. Obsahuje mód skramblovania (CAMode) a pole návesti zdieľaného skramblera (SharedFlag).

Formát a kódovanie: Pole CAOrg má dĺžku 16 bitov; používa sa tento formát:



Obrázok 8 – Formát poľa usporiadania CA (CAOrg

Umiestnenie: Usporiadanie CA sa môže prenášať v rôznych polohách, ako sa podrobne uvádza v príslušných článkoch.

5.4.1 Mód podmieneného prístupu (CAMode)

Aktuálne aplikovaný mód skramblovania sa nazýva CAMode.

Formát a kódovanie: Dĺžka je 3 bity.

000:	subkanál		CA;
001:	dátová	skupina	CA;
010:	MOT		CA;
011:	vlastníctvo		CA;
100:	rezervované;		
101:	rezervované;		
110:	rezervované;		
111:	rezervované.		

Umiestnenie: Prenáša sa v poli CAOrg.

5.4.2 Pole návesti zdieľaného skramblera (SharedFlag)

Pole návesti zdieľaného skramblera (SharedFlag) zodpovedá skramblovanému obsahu. Indikuje systém CA, ktorý sa môže použiť na deskramblovanie obsahu.

Formát a kódovanie: Návesť zdieľaného skramblera má dĺžku 8 bitov. Môže teda označovať až 8 rozličných systémov CA pracujúcich paralelne v rámci jednej služby.

Nie je nastavená nijaká návesť: neplatné.

Jedna návesť je nastavená: Neaplikuje sa nijaký systém zdieľaného skramblera (SSS); na deskramblovanie obsahu sa môže použiť príslušný systém CA.

Dve až osem návestí je nastavených: SSS je aplikovaný; dva až osem systémov CA spoločne poskytuje skramblovaný obsah a ktorýkoľvek z nich sa môže použiť na deskramblovanie obsahu.

Obrázok 9 – Kódovanie poľa návesti zdieľaného skramblera

Umiestnenie: Prenášaný je v poli CAOrg.

5.5 Indikácia usporiadania CA – CAOrgFlag/CAOrgIndi

Usporiadanie CA (CAOrg) obsahuje generickú informáciu o aplikovanom móde skramblovania a o systémoch CA, ako sa opisuje predtým. Jej existencia je indikovaná vlastným CAOrgFlag alebo implicitne existenciou poľa indikátora usporiadania CA (CAOrgIndi).

Formát a kódovanie:

Každá kombinácia indikátora CA a indikátora usporiadania CA má význam podľa zoznamu uvedeného ďalej:

Indikácia CA CAFlag/CAIndi	Indikácia usporiadania CA CAOrgFlag/CAOrgIndi	
0 /nie je prezentovaná	0 /nie je prezentovaná	nie je skramblovaná
0 /nie je prezentovaná	1 /prezentovaná	časť, ktorá korešponduje so skramblovaným obsahom
1 /prezentovaná	0 /nie je prezentovaná	porušená
1 prezentovaná	1 prezentovaná	výhradne korešponduje so skramblovaným obsahom

Umiestnenie: Umiestnenie indikácie usporiadania CA sa podrobne uvádza v príslušných článkoch.

5.6 Synchronizačné parametre CA (CASyncParam)

Okrem predtým uvedených parametrov, ktoré opisujú aplikované systémy CA a aplikovaný mód CA, na synchronizáciu deskramblera sú potrebné ďalšie parametre. Sú závislé od systému CA a nazývajú sa synchronizačné parametre CA (CASyncParam).

Minimálne to môže byť riadiaca návesť, ktorá indikuje zmenu riadiaceho slova. Môžu sa použiť aj iné parametre, ako počítadlo rámcov, inicializačný modifikátor a ďalšie. Príloha E uvádza prehľad možných synchronizačných parametrov.

Formát a kódovanie: Formát a kódovanie synchronizačných parametrov sa v tejto technickej špecifikácii nenormalizujú.

Umiestnenie: V závislosti od rôznych módov skramblovania sa synchronizačné parametre CA (CASyncParam) prenášajú v rôznych pozíciách, ako sa detailne opisuje v príslušných článkoch.

5.7 Podmienený prístup k systému vnútorných správ (CAIntMess)

Špecifické subpolia systému CA, ktoré sú v jednotlivých prípadoch CA rôzne, nazývajú sa subpolia podmieneného prístupu k systému vnútorných správ (CAIntMess). Tieto subpolia môžu obsahovať informácie manažovania, ktoré sa vzťahujú na oprávnenia používateľa a transportné kľúče, alebo môžu obsahovať aktuálne riadiace slovo a aktivovať kontrolu oprávnenia na strane prijímača. Prvé tri bity každého prenášaného subpoľa CAIntMess sú ShortCASysId. Takto sa stáva priradenie k systému CA jedinečným a tým sa umožňuje aplikácia SSS.

Formát a kódovanie: Formát a kódovanie sa v tejto technickej špecifikácii nenormalizujú.

Umiestnenie: V závislosti od rôznych módov skramblovania sa subpolia podmieneného prístupu k systému vnútorných správ (CAIntMess) prenášajú v rôznych pozíciách, ako sa detailne opisuje v príslušných článkoch.

5.8 Prehľad umiestnenia parametrov

Tabuľka 1 udáva prehľad umiestnenia predtým uvedených parametrov v multiplexe DAB v kombinácii troch módov CA: subkanál CA, dátová skupina CA a MOT CA.

Podrobnejšie informácie o kódovaní a úplný opis módov CA sa uvádzajú v ďalších článkoch. Príklady nastavenia parametrov v multiplexe DAB sa uvádzajú v prílohe B.

Tabuľka 1 – Prehľad umiestnenia parametrov opísaných v tomto článku v každom z troch módov skramblovania: subkanál CA, dátová skupina CA a objekty MOT CA

<table>
<tr><th rowspan="2"></th><th colspan="3" rowspan="2">Subkanál CA</th><th colspan="2">Dátová skupina CA</th><th colspan="2">Objekty MOT CA</th></tr>
<tr><th>Mód paketu</th><th>PAD</th><th>Vybraté objekty MOT sú skramblované</th><th>Všetky objekty MOT v dátovom karuseli MOT sú skramblované (pozri poznámku)</th></tr>
<tr><td>CAId</td><td colspan="3">FIG 0/2</td><td>FIG 0/2</td><td>-</td><td>FIG 0/2/-</td><td>FIG 0/2/-</td></tr>
<tr><td>CASysIdList</td><td colspan="3">FIG 6</td><td>FIG 6</td><td>FIG 6</td><td>FIG 6</td><td>FIG 6</td></tr>
<tr><td rowspan="2">CA Indication</td><td colspan="3">CAFlag v FIG 0/2</td><td rowspan="2">CAFlag
v
FIG 0/2</td><td rowspan="2">CAFlag
v
FIG 0/13</td><td colspan="2">CAIndi:
CAInfo existuje záhlavie MOT v zozname parametrov MOT</td></tr>
<tr><td>Packet Ch</td><td>Stream Ch</td><td>Audio Ch</td><td>CAFlag v FIG0/2/FIG 0/13</td></tr>
<tr><td>CAOrg Indication</td><td>CAOrgFlag v FIG 0/3</td><td>CAOrgIndi: existuje FIG 0/4</td><td>CAOrgIndi: existuje FIG 0/4</td><td>CAOrgFlag v FIG 0/3</td><td>CAOrgFlag v FIG 0/13</td><td colspan="2">CAIndi:
CAInfo existuje záhlavie MOT v zozname parametrov MOT</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>CAOrgFlag v FIG 0/3/FIG0/13</td></tr>
<tr><td>CAOrg
"povolené CAMode"</td><td>FIG 0/3
"subkanál CA" alebo "vlastníctvo CA"</td><td>FIG 0/4
"subkanál CA" alebo "vlastníctvo CA"</td><td>FIG 0/4
"subkanál CA" alebo "vlastníctvo CA"</td><td>FIG 0/3
"dátová skupina CA" alebo "vlastníctvo CA"</td><td>FIG 0/13
"dátová skupina CA" alebo "vlastníctvo CA"</td><td colspan="2">parameter CAInfo záhlavia MOT v zozname "MOT CA" alebo v zozname "vlastníctvo CA"</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>FIG 0/3 / FIG0/13 "MOT CA" alebo "vlastníctvo CA"</td></tr>
<tr><td>CASyncParam</td><td colspan="3">SUBCAPrefix</td><td colspan="2">DGCAPrefix</td><td colspan="2">MOTCAPrefix</td></tr>
<tr><td>CAIntMess</td><td colspan="3">SUBCAPrefix</td><td colspan="2">dátová skupina MSC typu 1</td><td colspan="2">číslo v zozname MOT
alebo
dátová skupina MSC typu 1</td></tr>
<tr><td colspan="8">POZNÁMKA. – V prípade, keď sú skramblované všetky objekty MOT dátového karuselu MOT (pozri EN 301 234 [2]), nemá zmysel prestavovať dátový karusel koncových zariadení bez možnosti CA. Tento prípad sa môže dodatočne signalizovať na tej istej úrovni ako dátová skupina CA takto:
o CAFlag v FIG0/2 alebo FIG 0/13 sú nastavené;
o CAOrgFlag v FIG0/3 alebo FIG 0/13 sú nastavené;
CAOrg v FIG0/3 alebo FIG 0/13, ktoré obsahujú kópiu CAOrg, sú prenášané v záhlaví MOT poľa CAInfo v zozname MOT.</td></tr>
</table>

6 Subkanál CA

Subkanál CA poskytuje najuniverzálnejší skramblovací mód a pokrýva veľký počet aplikácií. Pretože je umiestnený v transportnej vrstve, skrambluje kompletný subkanál MSC (napríklad nie je možné skramblovať dáta PAD bez skramblovania príslušného audioprogramu).

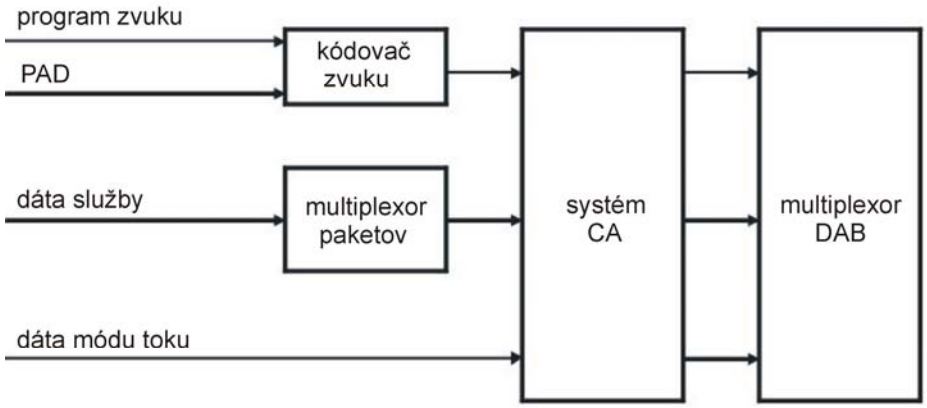
Vstupný tok:

– subkanál AUDIO s možným obsahom dát PAD;
– subkanál v paketovom móde, ktorý prenáša dátové služby v paketovom móde;
– subkanál v móde toku prenáša dáta v móde toku.

POZNÁMKA. – Keď je aplikovaný subkanál CA, rovnaké zabezpečenie proti chybám (EEP) sa javí ako opodstatnené nielen do kanálov s paketovým módom a módom toku, ale aj do subkanálov zvuku. To môže spôsobovať ďalšie zaťaženie.

6.1 Umiestnenie systému CA

Umiestnenie systému CA, ktorý predstavuje subkanál CA, je zobrazené na obrázku 10.



Obrázok 10 – Umiestnenie systému CA do subkanála CA

6.2 Signalizácia CA

Signalizácia subkanála CA sa vykonáva podľa koncepcie opísanej predtým. Signalizačné parametre sa prenášajú takto:

CAId: pozri čl. 5.1.

CASysIdList: pozri čl. 5.2.

CAFlag: pozri čl. 5.3.

V definícii komponenta služby FIG 0/2 (pozri čl. 6.3.1 EN 300 401 [1]) je návesť CAFlag nastavená na každý komponent služby.

CAOrg Indikátor, CAOrg: pozri čl. 5.4 a 5.5.

– **Subkanál v paketovom móde:** Ak je vstupným tokom subkanál v paketovom móde, potom sú CAOrgFlag a CAOrg prenášajú v komponente služby v paketovom móde s

podmieneným prístupom alebo bez podmieneného prístupu FIG 0/3 (pozri čl. 6.3.2 EN 300 401 [1]).

– **Subkanál AUDIO alebo subkanál módu toku:** Ak je vstupným tokom subkanál AUDIO alebo subkanál v móde toku, potom CAOrg je indikovaný implicitne existenciou CAOrgIndi: FIG 0/4. CAOrg sa prenáša v komponente služby s podmieneným prístupom v móde toku FIG 0/4 (pozri čl. 6.3.3 EN 300 401 [1])

CAMode: Pri rôznych transportných mechanizmoch sú definované parametrom TMId v opise komponenta služby FIG 0/2 (pozri čl. 6.3.1 EN 300 401 [1]), dovolené módy CA sa uvádzajú ďalej:

Transportný mechanizmus	TMId	CAMode	Význam
zvukový tok MSC	00	000	subkanál CA
	00	011	špeciálny mechanizmus CA
tok dát MSC	01	000	subkanál CA
	01	011	špeciálny mechanizmus CA
FIDC	10	v tejto technickej špecifikácii nie je normalizovaný	
paketizované data MSC	11	000	subkanál CA
	11	011	špeciálny mechanizmus CA

Subkanál CA nepokrýva FIDC. Na FIDC sa môže aplikovať špeciálny mechanizmus CA.

6.3 Prenos obsahu a subpolí CAIntMess

Subpolia CAIntMess sa prenášajú v tom istom subkanáli ako skramblovaný obsah, takže CAIntMess a skramblovaný obsah sa môžu jednoducho synchronizovať, čo je podstatné na oznámenie zmeny riadiaceho slova.

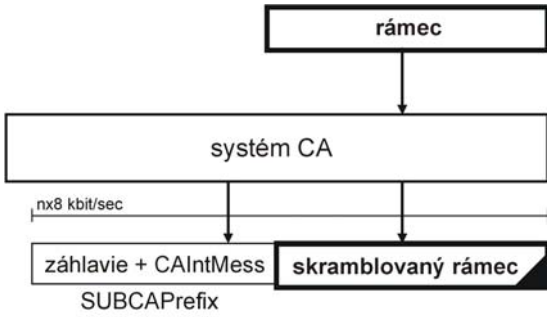
Subpolia CAIntMess sa prenášajú vnútri poľa, ktoré predchádza skramblovaný obsah. Toto pole sa nazýva prefix subkanála CA (SubCAPrefix). Dĺžka poľa SubCAPrefix je variabilná, čo vedie k narastajúcej bitovej rýchlosti subkanála:

– Ak je kapacita subkanála násobkom rýchlosti 8 kbit/s tak, ako je to pri subkanáli v paketovom móde alebo pri subkanáli AUDIO, potom sa môže zvýšiť len o 8 kb/s alebo o násobok 8 kb/s, čoho výsledkom je prídavná dĺžka rámca 24 bajtov alebo násobok 24 bajtov.

– Ak používateľská aplikácia módu toku nevyžaduje násobok rýchlosti 8 kb/s, potom prefixová informácia môže byť menšia, ako je násobok rýchlosti 8 kbps, za predpokladu, že súčet bitovej rýchlosti prefixových informácií a skramblovaný obsah je násobkom rýchlosti 8 kb/s.

POZNÁMKA. – Typická kapacita audiokanála 160 kbit/s vyžaduje pridanie 8 kbit/s a zvýšenie zaťaženia CA o 5 % a dĺžky SUBCAPrefix o 24 bajtov. Typická kapacita dátového kanála 64 kbit/s vyžaduje pridanie 8 kbit/s a zvýšenie zaťaženia CA o 12,5 % a dĺžky SUBCAPrefix o 24 bajtov.

Polia CAIntMess sa podelia na pakety a prenesú sa vnútri polí SubCAPrefix v ďalších rámcoch. Z toho dôvodu sa musí definovať záhlavie rámca.



Obrázok 11 – Prenos obsahu a subpolí CAIntMess

6.4 Kódovanie prefixu SUBCA

Štruktúra a kódovanie prefixu SUBCA sa v tejto technickej špecifikácii nenormalizujú. V prílohe G sa uvádza odporúčanie. Poskytovatelia CA, ktorí aplikujú SSS, použijú jednotnú štruktúru prefixu SUBCA.

7 Dátová skupina CA

Dátová skupina sa prenáša v subkanáli paketového módu alebo v PAD.

Dátové skupiny prenášané v subkanáli paketového módu:

Dátová skupina CA:

– skrambluje každú dátovú skupinu komponenta služby, z čoho vyplýva, že sú skramblované aj dátové skupiny, ktoré obsahujú manažovacie dáta MOT (zoznam MOT, záhlavie MOT);

– skrambluje len niektoré skupiny komponenta služby; prijímač bez možnosti CA môže spracovať neskramblované dátové skupiny zodpovedajúceho komponenta služby, napríklad vo vloženej aplikácii IP sa obraz môže skramblovať, ale zvuk sa nemusí skramblovať.

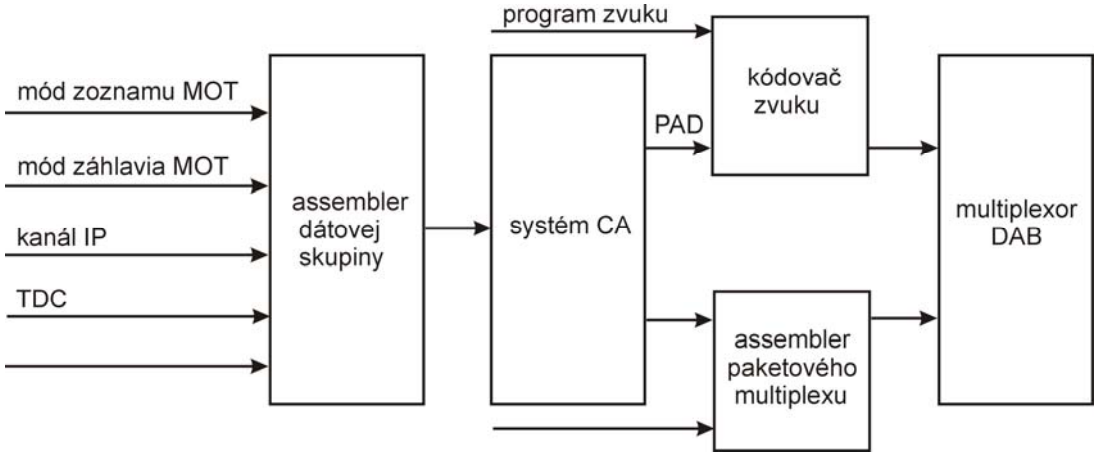
Dátové skupiny prenášané v PAD:

Dátová skupina CA:

– skrambluje všetky dáta používateľskej aplikácie; prijímač bez možnosti CA nemôže prezentovať nič z používateľskej aplikácie;

– skrambluje len časť dát používateľskej aplikácie, napríklad niektoré zábery prezentácie (SLS) sú skramblované a iné zostávajú neskramblované; prijímač bez možnosti CA môže prezentovať neskramblované časti používateľskej aplikácie.

7.1 Umiestnenie systému CA



Obrázok 12 – Umiestnenie systému CA dátovej skupiny CA

7.2 Signalizácia

Signalizácia dátovej skupiny CA sa vykonáva podľa predtým opísanej koncepcie. Musí sa rozlišovať medzi dátovými skupinami prenášanými v subkanáli paketového módu a dátovými

skupinami prenášanými v PAD. Signalizačné parametre sa prenášajú rôznymi spôsobmi v každom z prípadov.

7.2.1 Signallizácia dátových skupín prenášaná v subkanáli paketového módu

CAId: pozri čl. 5.1.

CASysIdList: pozri čl. 5.2.

CAFlag: pozri čl. 5.3 a 6.2. Návesť CAFlag je nastavená na mód definície komponenta služby FIG 0/2 (pozri čl. 6.3.1 EN 300 401 [1]) s každým úplne skramblovaným komponentom služby.

CAOrg Indikátor, CAOrg: pozri čl. 5.4, 5.5 a 6.2. Návesti CAOrgFlag a CAOrg sa prenášajú do komponenta služby v paketovom móde s podmieneným prístupom alebo bez podmieneného prístupu FIG 0/3 (pozri čl. 6.3.2 EN 300 401 [1]).

CAMode: Dovolený mód CAMode sa definuje takto:

001: dátová skupina CA; 011: vlastníctvo CA.

Záhlavie paketu – Príkaz: Ako vysvetľuje čl. 5.3.2 v EN 300 401 [1], príkazová návesť v záhlaví paketu indikuje význam paketu. Identifikuje, či sa paket používa na neskramblované dátové skupiny alebo na skramblované dátové skupiny a dátové skupiny, ktoré obsahujú podmienený prístup k systému vnútorných správ (CAIntMess) týmto spôsobom:

0: paket sa nevzťahuje na CA: môže sa použiť ako obyčajný;

1: paket súvisí s CA (skramblované dátové skupiny alebo dátové skupiny, ktoré obsahujú podmienený prístup k systému vnútorných správ): musí sa spracovať subsystémom CA.

Návesť príkazu sa nastavuje do paketov obsahujúcich skramblované dátové skupiny MSC, ako aj do paketov, ktoré obsahujú polia TCAIntMess (dátová skupina MSC typu 1).

Koncové zariadenie, ktoré nesúvisí s CA, ignoruje pakety s návesťou príkazu nastavenou na 1.

7.2.2 Signalizácia dátovej skupiny prenášanej v PAD

CAId: Neexistuje, keď sa dátové skupiny prenášajú v PAD, FIG 0/2 sa nepoužíva.

CASysIdList: pozri čl. 5.2.

CAFlag, CAOrgFlag, CAOrg: pozri čl. 5.3, 5.4 a 5.5.

Návesti CAFlag, CAOrgFlag a CAOrg sa prenášajú v poli dáta používateľskej aplikácie PAD FIG 0/13 (pozri čl. 8.1.20 EN 300 401 [1]).

CAMode: Dovolený mód CAMode sa definuje takto:

001: dátová skupina CA;
011: vlastníctvo CA.

Typ aplikácie X-PAD: Nastavenie typu aplikácie X-PAD FIG 0/13 indikuje význam paketu; identifikuje, či sa paket používa pri neskramblovaných dátových skupinách alebo pri skramblovaných dátových skupinách a dátových skupinách, ktoré obsahujú podmienený prístup k systému vnútorných správ (CAIntMess,) týmto spôsobom:

Nastavenie	Význam
+0, +1	paket nesúvisiaci s CA: môže sa spracovať ako obyčajný
+2, +3	paket súvisiaci s CA; skramblované dátové skupiny alebo dátové skupiny, ktoré obsahujú pole podmieneného prístupu k systému vnútorných správ: musia prejsť cez subsystém CA

Nastavenie je +2 alebo +3 a pole CAOrg je prítomné v paketoch, ktoré obsahujú skramblované dátové skupiny MSC, ako aj v paketoch, ktoré obsahujú polia CAIntMess (dátová skupina MSC typu 1).

Koncové zariadenie, ktoré nesúvisí s CA, spracúva len pakety označené nastavením +0 alebo +1.

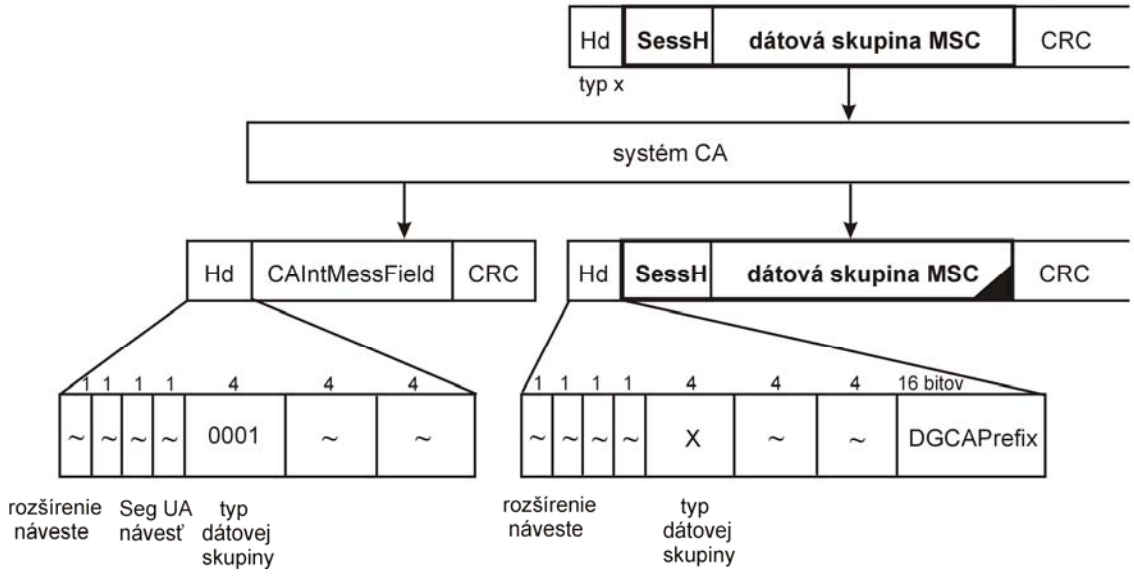
Koncové zariadenie, ktoré súvisí s CA, spracúva pakety označené nastavením +0 a +1, ako aj pakety označené nastavením +2 alebo +3.

> PRÍKLAD. – Prezentácia: ak typ aplikácie s najnižším číslom použitý na prenos tejto používateľskej aplikácie je 12, potom neskramblované záhlavie MOT, ako aj neskramblované telo MOT používajú aplikáciu X-PAD typu 12/13; skramblované záhlavie MOT, skramblované telo MOT, ako aj subpolia CAIntMess používajú aplikáciu X-PAD typu 14/15.

7.3 Prenos obsahu CAIntMess a subpolí CAIntMess

Skramblovanie dátovej skupiny MSC pozostáva zo skramblovania záhlavia sekcie spolu s dátovou skupinou MSC dátového poľa. Začiatočné záhlavie dátovej skupiny MSC zostáva neskramblované a je nahradené prefixom dátovej skupiny CA (DGCAPrefix). Nová dátová skupina CRC kanála, ak sa poskytuje, vypočíta sa z nastaveného záhlavia dátovej skupiny MSC a skramblovanej dátovej skupiny MSC.

Subpolia podmieneného prístupu k systému vnútorných správ (CAIntMess) a ďalšie informácie riadenia systému a manažovania sa takisto prenášajú v dátových skupinách MSC (pozri čl. 5.3.3.1 EN 300 401 [1]). Subpolia CAIntMess a skramblovaný obsah sa môžu ľahko synchronizovať.



Obrázok 13 – Prenos obsahu CAIntMess a subpolí CAIntMess

7.3.1 Prenos obsahu CAIntMess

Záhlavie sekcie dátovej skupiny MSC je skramblované spolu s dátami dátovej skupiny MSC.

Pole DGCAPrefix predchádza skramblovanému obsahu.

Záhlavie dátovej skupiny MSC: Záhlavie dátovej skupiny MSC sa definuje takto:

– Rozšírená návesť: Táto jednobitová návesť indikuje prítomnosť DGCAPrefix takto:

0: DGCAPrefix nie je prezentované;
1: DGCAPrefix je prezentované.

– Typ dátovej skupiny: Štvorbitové pole obsahuje typ prenášanej dátovej skupiny MSC; typ dátovej skupiny skramblovanej dátovej skupiny MSC je rovnaký ako typ dátovej skupiny neskramblovanej dátovej skupiny.

– DGCAPrefix: Použitie a kódovanie dvojbajtového poľa nie je normatívne;

ostatné polia v záhlaví dátovej skupiny MSC sú nastavené špecificky.

Záhlavie sekcie: Záhlavie sekcie dátovej skupiny MSC je skramblované spolu s dátami dátovej skupiny MSC.

Dátové pole dátovej skupiny MSC: Dáta dátovej skupiny MSC sú skramblované spolu so záhlavím sekcie dátovej skupiny MSC.

Dátová skupina CRC kanála MSC (ak je prezentovaná): Dátová skupina CRC skramblovanej dátovej skupiny MSC je vypočítaná z nastaveného záhlavia dátovej skupiny MSC a skramblovanej dátovej skupiny MSC (záhlavie sekcie spolu s dátovým poľom dátovej skupiny MSC) a je generovaná podľa procedúry definovanej v čl 5.3.3.3 EN 300 401 [1].

7.3.2 Prenos subpolí CAIntMess

Subpolia CAIntMess sa prenášajú v poli CAIntMessField, ktoré je umiestnené v dátovom poli dátovej skupiny, ktorá patrí do inej dátovej skupiny MSC typu 1.

Subpolia CAIntMess sa môžu prenášať ako celok.

Záhlavie dátovej skupiny MSC: definované takto:

– Typ dátovej skupiny Data Group Type: štvorbitové pole, ktoré obsahuje typ prenášanej dátovej skupiny MSC; typ dátovej skupiny je 0001.

Ostatné polia v záhlaví dátovej skupiny MSC sú nastavené špecificky.

7.4 Kódovanie poľa CAIntMessField

Pole CAIntMessField obsahuje subpole podmieneného prístupu k systému vnútorných správ (CAIntMess). Odporúča sa prenos úplného subpoľa CAIntMess v rámci jedného poľa CAIntMessField.

Budúce použitie, štruktúra a kódovanie poľa CAIntMessField sú špecifické v systéme CA a môžu sa navzájom líšiť.

Okrem subpoľa podmieneného prístupu k systému vnútorných správ (CAIntMess) sa tu môžu umiestniť tieto parametre:

ShortCASysId: Ako sa vysvetľuje v čl. 4.4 a v čl. 5.2.2: na realizáciu koncepcie so zdieľaným skramblerom, každé subpole správ CAIntMess prenášané v poli CAIntMessField sa začína nejakým ShortCASysId.

Riadenie komunikácie CA: pozri prílohu E.

7.5 Kódovanie poľa DGCAPrefix

Prítomnosť poľa DGCAPrefix je voliteľná a indikovaná nastavením návesti rozšírenia na1. Jeho použitie, štruktúra a kódovanie sa v tejto technickej špecifikácii nenormalizujú.

Synchronizačné parametre CA CASyncParam (pozri prílohu E) sa môžu prenášať v poli DGCAPrefix.

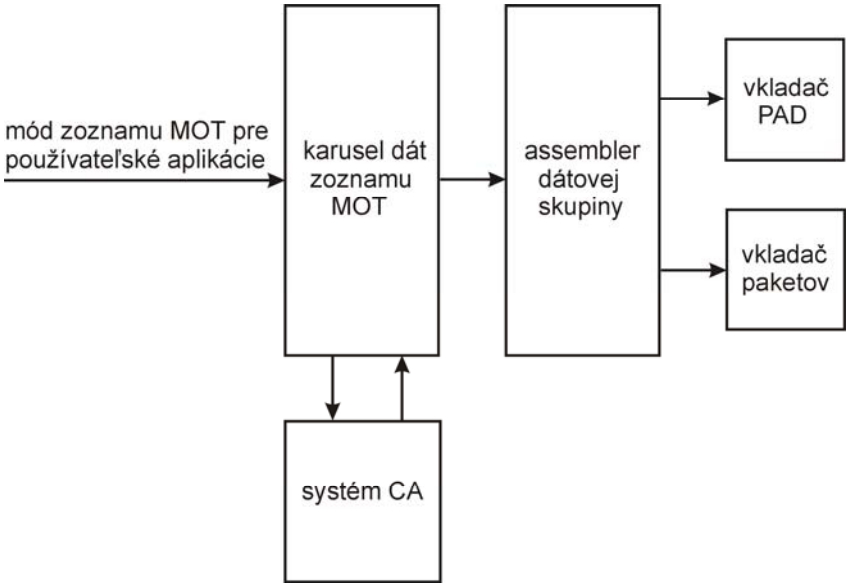
8 MOT CA

MOT CA sa vťahuje na mód zoznamu MOT. Vykonáva skramblovanie niektorého alebo všetkých objektov MOT v štruktúre zoznamu. Zoznam MOT zostáva neskramblovaný.

Prijímač bez CA môže stále spracúvať neskramblované objekty. Napríklad v aplikácii BWS neskramblované strany sa môžu stať vstupnými stranami alebo môžu obsahovať informáciu, ako si predplatiť službu, a niektoré ukážky dát.

Informácie o tom, ktoré objekty sú skramblované a ktoré zostávajú neskramblované, nachádzajú sa v zozname MOT. Zoznam MoT zostáva neskramblovaný.

8.1 Umiestnenie systému CA



Obrázok 14 – Umiestnenie systému CA System MOT CA

8.2 Signalizácia CA

Signalizácia MOT CA sa vykonáva podľa koncepcie uvedenej predtým.

CAId: pozri článok 5.1.

CASysIdList: pozri článok 5.2.

Indikácia CA

Nepoužíva sa presná návesť CAFlag. Indikácia CA je daná parametrom CAIndi, v prípade MOT CA je to existencia MOT parametra CAInfo (0 × 23), čo je časť informácie záhlavia MOT (pozri čl. 6.2.2.3.1 EN 301 234 [2]). Tento parameter indikuje, že telo príslušného objektu MOT je skramblované.

Každý dekódovač MOT má kontrolovať existenciu parametra CaInfo MOT.

– Prijímač bez CA nevyhodnocuje obsah parametra CAInfo MOT a nespracúva príslušný objekt MOT.

– Prijímač s CA vyhodnocuje obsah parametra CAInfo MOT, aby rozhodol, či je schopný pokračovať v spracúvaní príslušného objektu MOT.

Indikácia CAOrg

Nepoužíva sa presná návesť CAOrgFlag. Indikácia CAOrg je daná CAOrgIndi, v prípade MOT CA je to existencia parametra CAInfo MOT (0x23), čo je časť informácie záhlavia MOT(pozri čl. 6.2.2.3.1 EN 301 234 [2]). Tento parameter indikuje, že CAOrg je prítomný ako jeden z parametrov v parametri CAInfo MOT.

Každý dekódovač MOT má kontrolovať existenciu parametra CAInfo MOT:

– prijímač bez CA nevyhodnocuje obsah parametra CAInfo MOT a nespracúva príslušný objekt MOT;

– prijímač s CA vyhodnocuje obsah parametra CAInfo MOT a vyhodnocuje pole CAOrg, aby rozhodol, či je schopný pokračovať v spracovaní príslušného objektu MOT.

Ak sú všetky objekty MOT a dátový karusel MOT skramblované, s koncovým zariadením bez CA je prestavba dátového karusela MOT neopodstatnená.

Takýto prípad sa môže dodatočne signalizovať takto:

– návesť CAFlag v FIG0/2 alebo FIG 0/13 je nastavená;

– návesť CAOrgFlag v FIG0/3 alebo FIG 0/13 je nastavená;

– CAOrg vo FIG0/3 alebo FIG 0/13 obsahuje kópiu CAOrg prenášanú v parametri CAInfo MOT poľa v zozname MOT.

Mód CA: Dovolený mód CA sa definuje takto:

010: MOT CA;
011: vlastníctvo CA.

Identifikácia:

Dátové skupiny prenášané v subkanáli s paketovým módom:

– Pakety obsahujúce dátové skupiny MSC so skramblovanými segmentmi tela MOT (dátová skupina MSC typ 5), ako aj pakety obsahujúce CAIntMess a prenášané v dátovej skupine MSC typu 1 sú indikované nastavením riadiacej návesti v záhlaví paketu.

– Zoznam MOT, ktorý obsahuje neskramblované záhlavia MOT a ktorý sa prenáša v dátovej skupine MSC typu 6 alebo typu 7, ako aj dátové skupiny MSC typu 4 s neskramblovaným obsahom sa prenášajú v paketoch, kde je riadiaca návesť nastavená na 0.

Koncové zariadenie bez CA ignoruje pakety indikované nastavenou návesťou.

Dátové skupiny prenášané v PAD:

Subpolia X-PAD, ktoré obsahujú dátové skupiny MSC so skramblovanými telami segmentov MOT (dátová skupina typu 5), ako aj subpolia X-PAD, ktoré obsahujú CAIntMess a prenášajú sa v dátovej skupine MSC typu 1, sú indikované posunom typu aplikácie X-PAD +2 alebo+3.

Zoznam MOT, ktorý obsahuje neskramblované záhlavia MOT a ktorý sa prenáša v dátovej skupine MSC typu 6 alebo typu 7, ako aj iné dátové skupiny MSC typu 4 s neskramblovaným obsahom sa prenášajú v subpoliach X-PAD, kde je posuv typu aplikácie X-PAD +0 alebo+1.

Koncové zariadenie bez CA spracúva len subpolia X-PAD indikované posunom +0 alebo +1. Koncové zariadenie CA spracúva subpolia X-PAD indikované posunom +0 a +1, ako aj subpolia X-PAD indikované posunom +2 alebo +3.

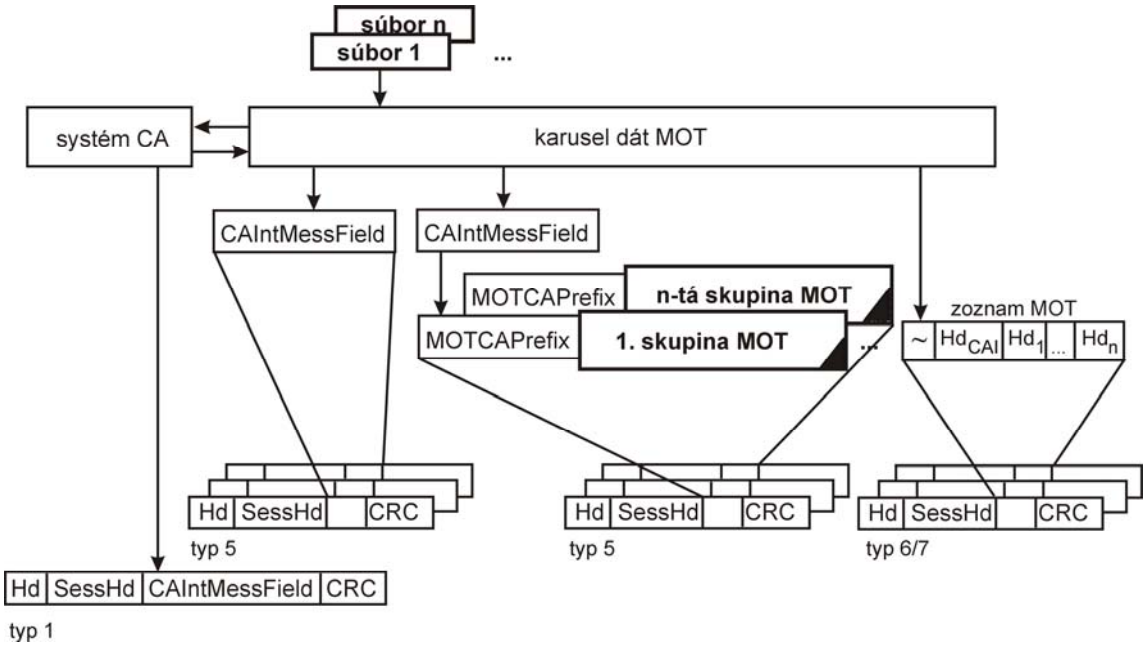
PRÍKLAD. – Webová stránka vysielania: Ak typ aplikácie s najnižším číslom používaný na prenos tejto používateľskej aplikácie je 12, potom neskramblovaný zoznam MOT, ako aj neskramblované telá MOT používajú aplikáciu X-PAD typu 12/13. Skramblované telá MOT, ako aj subpolia CAIntMess používajú aplikáciu X-PAD typu 14/15.

8.3 Prenos obsahu CAIntMess a subpolí CAIntMess

MOT CA sa vzťahuje na mód zoznamu MOT. Umožňuje skramblovanie vybraných častí MOT v štruktúre zoznamu.

Informáciu, ktoré objekty sú skramblované a ktoré zostávajú neskramblované, obsahuje zoznam MOT. Zoznam MOT zostáva neskramblovaný.

Subpolia CAIntMess sa môžu prenášať v tele MOT, alebo v poli dátovej skupiny MSC nejakej dátovej skupiny MSC typu 1.



Obrázok 15 – Prenos obsahu CAIntMess a subpolí CAIntMess

8.3.1 Prenos obsahu CAIntMess

Zoznam MOT, ktorý takisto obsahuje záhlavia MOT, zostáva neskramblovaný. Prenáša sa v dátovej skupine MSC typu 6 alebo typu 7.

Skramblované telá MOT sa prenášajú v dátových poliach dátovej skupiny MSC dátovej skupiny typu 5.

Každému skramblovanému telu MOT má predchádzať pole MOTCAPrefix. MOTCAPrefix je potom časťou tela MOT.

8.3.2 Prenos subpolí CAIntMess

Subpolia CAIntMess sa prenášajú v poli CAIntMessField:

– Toto pole sa môže umiestniť v dátovom poli dátovej skupiny MSC dátovej skupiny MSC typu 1.

– Je umiestnené v tele MOT a bude sa prenášať v dátových poliach dátovej skupiny MSC dátovej skupiny MSC typu 5.

– Je umiestnené v poli MOTCAPrefi, ktoré predchádza skramblovaný obsah a je časťou tela MOT, ktoré sa prenáša v dátových poliach dátovej skupiny MSC dátovej skupiny MSC typu 5.

Ktorá z troch možností prenosu subpolí CAIntMess sa vyberie, závisí hlavne od týchto ďalších aspektov:

Prenos subpolí CAIntMess v dátovej skupine MSC typ 1: Dátové pole dátovej skupiny MSC typu 1 sa môže použiť CAIntMess obsahujúce informáciu manažérstva CA, ktorá nezávisí od obsahu.

Prenos subpolí CAIntMes v tele MOT v dátovej skupine MSC typu 5: Subpolia CAIntMess v tele MOT sú časťou dátového karusela zoznamu MOT; tieto subpolia CAIntMess sa považujú za súčasť obsahu.

Informácia záhlavia MOT objektu MOT, ktorá obsahuje pole CAIntMessField, sa prenáša spolu s ostatnými informáciami záhlavia MOT v zozname MOT:

– Ak sa subpolia CAIntMess vzťahujú na viac ako jedno skramblované telo MOT, môžu sa prenášať v samotnom tele MOT.

– Ak sa subpolia CAIntMess vzťahujú na jedno skramblované telo MOT, môže sa prenášať v poli MOTCAPrefix.

8.4 Kódovanie poľa CAIntMessField

Pole CAIntMessField obsahuje subpole podmieneného prístupu k systému vnútorných správ (CAIntMess). Odporúča sa prenos jedného úplného subpoľa CAIntMess v jednom poli CAIntMessField.

Ďalšie použitie, štruktúra a kódovanie sú špecifické v každom CA a môžu sa vzájomne odlišovať. Okrem subpoľa podmieneného prístupu k systému vnútorných správ (CAIntMess) sa tu môžu umiestniť tieto parametre:

ShortCASysId: Ako sa vysvetľuje v čl. 4.4 a čl. 5.2.2 na realizáciu koncepcie so zdieľaným skramblerom, každé subpole CAIntMess prenášané v poli CAIntMessField sa začína identifikátorom ShortCASysId.

Riadenie komunikácie CA: pozri prílohu E.

8.5 Kódovanie poľa MOTCAPrefix

Prítomnosť poľa MOTCAPrefix je voliteľná. Jeho štruktúra, použitie a kódovanie sú špecifické v systéme CA a nenormalizujú sa v tejto technickej špecifikácii.

Subpole CAIntMess, ktoré sa vzťahuje na skramblované telo MOT, ako aj synchronizačné parametre CA ShortCASysId (pozri prílohu E) sa môžu prenášať v poli MOTCAPrefix.

Príloha A (normatívna)

Príklad koncepcie so zdieľaným skramblerom

V jednej službe je použitých 5 rozličných systémov CA – A, B, C, D, E. Majú krátky identifikátor ShortCASysId s hodnotami 0 až 4. Príslušný zoznam CASysIdList sa uvádza ďalej. Pozostáva z 5 prvkov zoznamu.

ShortCASysId	CASysId	CAIntChar
000	CA System A	aaa
001	CA System B	bbb
010	CA System C	ccc
011	CA System D	ddd
100	CA System E	eee

V príklade sú 4 zložky služby W, X, Y a Z a sú spracované rôznymi spôsobmi:

– Zložka služby W je skramblovaná CA systému A (ShortCASysId = 0).
– Zložka služby X nie je vôbec skramblovaná.
– Zložka služby Y je skramblovaná CA systému B (ShortCASysId = 1).
– Zložka služby Z je skramblovaná prostredníctvom systému so zdieľaným skramblerom, kde CA systému B (ShortCASysId = 1), D (ShortCASysId = 3) a E (ShortCASysId = 4) pracujú synchronizovane.

Každá skramblovaná zložka služby je opísaná jej vlastným poľom CAOrg, ktoré obsahuje jej vlastnú návesť SharedFlag:

Zložka služby W: **SharedFlag** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
flags System A (ShortCASysId = 0)

Zložka služby X: **No SharedFlag**

Zložka služby Y: **SharedFlag** | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
flags System B (ShortCASysId = 1)

Zložka služby Z: **SharedFlag** | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
flags System B (ShortCASysId = 1)
flags System D (ShortCASysId = 3)
flags System E (ShortCASysId = 4)

Príloha B (informatívna)

Príklady nastavenia parametrov v multiplexe DAB

Signalizácia je znázornená v ďalších 9 príkladoch a uvádza sa v tabuľke ďalej:

PRÍKLAD:

1. Skramblovaný zvukový kanál:

Príklad skramblovania úplného subkanála a použitie subkanála CA.

2. Čiastočne skramblovaná dátová skupina aplikácie prenášaná v subkanáli s paketovým módom:

Skramblované sú len niektoré dátové skupiny zložky služby. Aplikuje sa dátová skupina CA. Môže sa vložiť aplikácia IP, kde obraz je skramblovaný, ale zvuk zostáva neskramblovaný.

3. Úplne skramblovaná dátová skupina aplikácie prenášaná v subkanáli s paketovým módom: Každá dátová skupina zložky služby je skramblovaná. Aplikuje sa dátová skupina CA.

4. Aplikácia MOT, kde sú skramblované vybraté objekty MOT, prenášané v subkanáli s paketovým módom:

Môže to byť časť webovej stránky vysielania (BWS). Aplikuje sa CA MOT.

5. Aplikácia MOT, kde sú skramblované všetky objekty MOT dátového karusela, prenášané v subkanáli s paketovým módom:

S koncovým zariadením bez CA nie je opodstatnená prestavba dátového karusela. CA sa môže signalizovať dodatočne na tej istej úrovni ako dátová skupina CA.

6. Čiastočne skramblovaná dátová skupina aplikácie prenášaná v PAD:

Časť dát používateľskej aplikácie je skramblovaná. Aplikuje sa dátová skupina CA. Môžu to byť napríklad nejaké snímky prezentácie (SLS), kým iné zostávajú neskramblované.

7. Úplne skramblovaná dátová skupina aplikácie prenášaná v PAD:

Všetky dáta používateľskej aplikácie sú skramblované dátovou skupinou CA.

8. Aplikácia MOT, kde sú skramblované vybraté objekty MOT, prenášané v PAD:

Môže to byť časť webovej stránky vysielania (BWS). Aplikuje sa CA MOT.

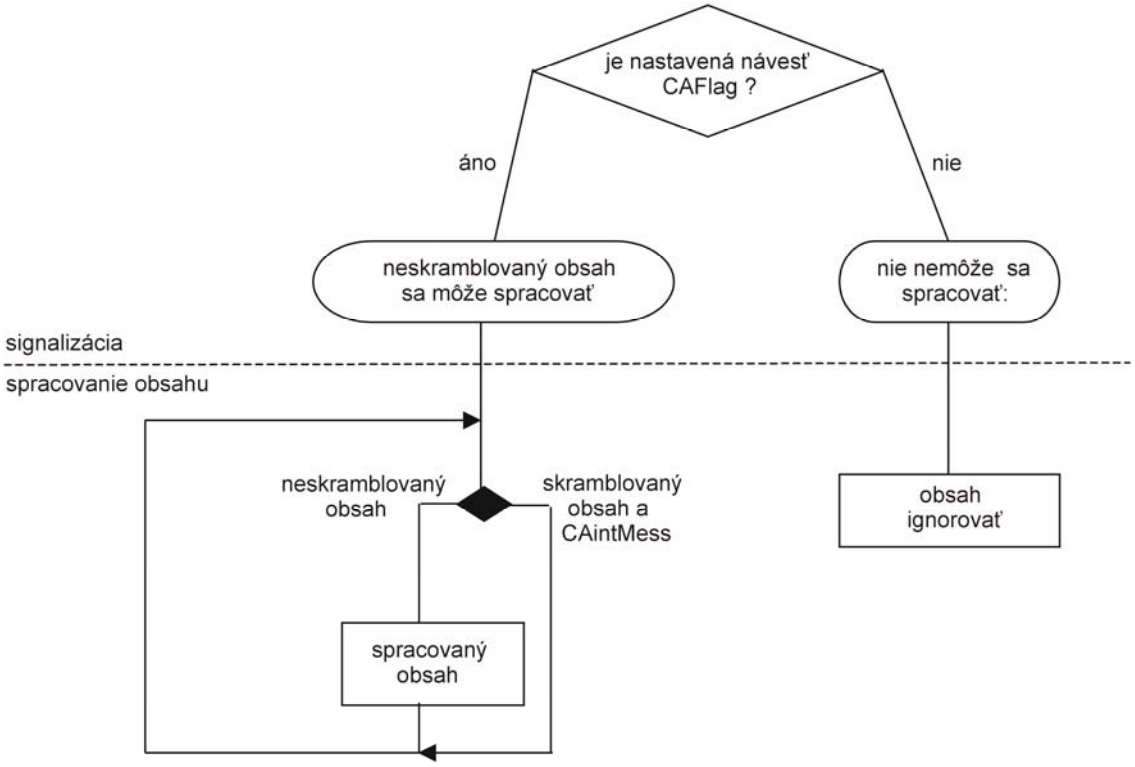
9. Aplikácia MOT, kde sú skramblované všetky objekty dátového karusela MOT prenášané v PAD. S koncovým zariadením bez CA nie je opodstatnená prestavba dátového karusela. CA sa môže signalizovať dodatočne na tej istej úrovni ako dátová skupina CA.

Príklad		1.	2.	3.	4.	5.	6.	7.	8.	9.
Transportované v:		Subkanál AUDIO	Mód paketu subkanála				PAD			
Aplikovaný mód CA:		Subkanál CA	Dátová skupina CA		MOT CA		Dátová skupina CA		MOT CA	
Signalizácia:		skramblovaný kanál AUDIO	skramblo-vaná časť skupiny dát aplikácie	skramblo-vané všetky skupiny dát aplikácie	výber objektov MOT na scramblo-vanie	skramblo-vané všetky objekty MOT dátového karusela v zozna-me MOT	skramblo-vaná časť skupiny dát aplikácie	skramblo-vané všetky skupiny dát aplikácie	výber objek-tov MOT na scram-blo-vanie	skramblo-vané všetky objekty MOT dátového karusela v zozna-me MOT
Par.	Parameter umiestne-nie	Nastavenie								
CA Id	FIG 0/2	111	111	111	111	111	-	-	-	-
CASys-IdList	existencia FIG 6	áno	áno	áno	áno	áno	áno	áno	áno	áno
Indikácia CA	CAFlag v FIG 0/2	1	0	1	0	1*)	-	-	-	-
	CAFlag v FIG 0/13	-	-	-	-	-	0	1	0	1*)
	existencia záhlavia MOT parametra CAInfo v zozname MOT	-	-	-	áno	áno	-	-	áno	áno
Indikácia CAOrg	CAOrgFlag v FIG 0/3	-	1	1	0	1*)	-	-	-	-
	existencia FIG 0/4	ano	-	-	-	-	-	-	-	-
	CAOrgFlag v FIG 0/13	-	-	-	-	-	1	1	0	1*)
	existencia záhlavia MOT parametra CAInfo v zozname MOT	-	-	-	áno	áno	-	-	áno	áno
CAOrg (CAMode)	FIG 0/3	-	dátová skupina CA	dátová skupina CA	-	MOT CA*)	-	-	-	-
	FIG 0/4	"subkanál CA"	-	-	-	-	-	-	-	-
	FIG 0/13	-	-	-	-	-	dátová skupina CA	dátová skupina CA	-	MOT CA*)
	záhlavie MOT parametra CAInfo v zozname MOT	-	-	-	MOT CA	MOT CA	-	-	MOT CA	MOT CA

nastavenie doplnkového parametra:		**dátová skupina typu hodnota MOT:** 5		**dátová skupina typu hodnota MOT:** 5
	záhlavie paketu – príkaz návesti: 1		**aplikácia typu posun X-PAD:** +2 alebo +3	
(-) Stav – umiestnený parameter nie je prezentovaný. *) Odporúčaná voliteľná signalizácia, zabraňuje koncovému zariadeniu bez možnosti CA prestaviť dátový karusel MOT len na detegovanie toho, že všetky objekty sú skramblované.				

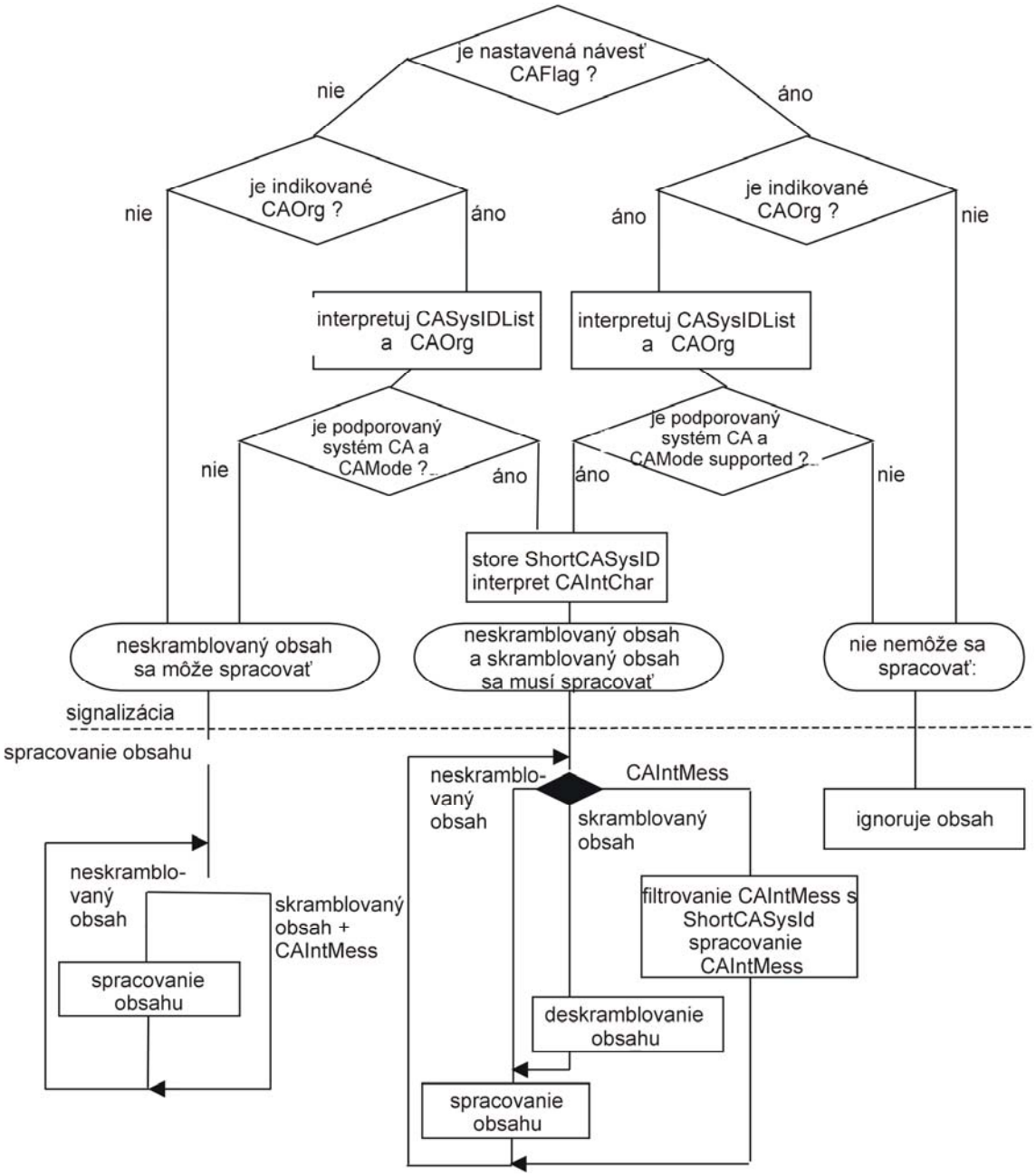
Príloha C (informatívna)

Fungovanie koncových zariadení bez CA



Príloha D (informatívna)

Fungovanie koncových zariadení s CA



.

Príloha E (informatívna)

Synchronizačné parametre

K parametrom uvedeným predtým, ktoré opisujú aplikovaný systém CA a aplikované módy CA, sú navyše potrebné parametre na synchronizáciu deskramblera. Nazývajú sa synchronizačné parametre CA (CASyncParam).

Minimom môže byť preklápacia návesť, ktorá indikuje zmenu riadiaceho slova, ale môžu sa použiť aj iné parametre, ako počítadlo rámcov, inicializačný modifikátor atď.

V ďalšom texte sa vysvetľujú niektoré možné parametre. Nenormalizujú sa v tejto technickej špecifikácii. Ich umiestnenie závisí od aplikovaného skramblovacieho módu.

Control Word Toggle (preklápacia návesť riadiaceho slova): Tento bit signalizuje aktuálne použité riadiace slovo, jeho označenie preklápacou návesťou indikuje zmenu riadiaceho slova.

Control Word Change Countdown (odpočet zmeny riadiaceho slova): V prípade subkanála CA odpočet zmeny riadiaceho slova indikuje počet zostávajúcich rámcov, kým nastane zmena riadiaceho slova. Používa sa na upozornenie vopred, že nastane zmena riadiaceho slova. Používanie a interpretácia odpočtu zmeny riadiaceho slova zvyšuje stabilitu systému.

Frame Counter (počítadlo rámcov): Stav počítadla rámcov sa zvyšuje s každým preneseným rámcom. Bolo by užitočné udržiavať deskrambler v koncovom zariadení v synchronizácii, ale jeho interpretácia s koncovými zariadeniami je voliteľná. Stav počítadla rámcov sa zvyšuje s každým preneseným a skramblovaným rámcom, jeho dĺžka má byť pevná. Preplnenie vedie k reštartu počítadla. Nie je potrebné prenášať počítadlo rámcov v každom rámci, ale tak často, ako je to potrebné na udržanie deskramblera v koncovom zariadení v synchronizácii.

Initialization Modifier (inicializačný modifikátor): K prenášanému riadiacemu slovu niektoré deskramblovacie algoritmy potrebujú navyše inicializačný modifikátor IM na reinicializáciu generátora pseudonáhodnej binárnej postupnosti a na umožnenie rýchlej synchronizácie skramblera a deskramblera.

Communication Controller (CA) [riadenie komunikácie (CA)]: Koncové zariadenie s viacnásobným kryptovaním obsahuje riadenie komunikácie CA (CACC) ako trvalú zložku a poskytuje možnosť pripojiť vymeniteľné moduly, napríklad karty smart a karty SIM, rôznych systémov CA. Riadenie komunikácie CA je nezávislé od systému CA. Ďalej sa musí definovať záhlavie CACC. Záhlavie CACC predchádza subpoľu CAIntMess, ale subpoľu CAIntMess predchádza aj skramblovaný obsah, ktorý obsahuje informácie typu, ako má koncové zariadenie narábať so skramblovaným obsahom alebo so subpoľom CAIntMess. CACC interpretuje tieto záhlavia.

Príloha F (normatívna)

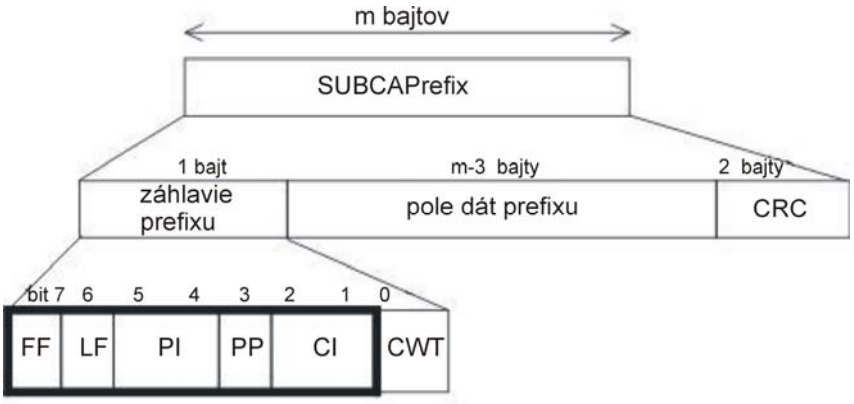
Identifikátor systému podmieneného prístupu (CASysID)

Tabuľka obsahuje hodnoty identifikátora systému podmieneného prístupu (CASysID). Pozri čl. 5.2.1.

CASysId (hexadecimal)	Systém podmieneného prístupu	Odkaz
0x8ECA	HECA vysoko efektívny podmienený prístup	Fraunhofer IIS http://www.iis.fraunhofer.de/dab/projects/heca/index.html T-Systems

Príloha G (informatívna)

Odporúčané kódovanie poľa SUBCAPrefix



Obrázok G.1 – Kódovanie poľa SUBCAPrefix

Dĺžka poľa SUBCAPrefix: Ako je vysvetlené predtým, dĺžka poľa SUBCAPrefix závisí od pridelenej bitovej rýchlosti použiteľnej v subpoli podmieneného prístupu k systému vnútorných správ. V ďalších položkách sa predpokladá dĺžka poľa m bajtov.

Štruktúra poľa SUBCAPrefix:

– záhlavie predvoľby 1 bajt;
– dátové pole predvoľby m – 3 bajty;
– CRC 2 bajty, cyklická kontrola redundancie.

(PRÍKLAD. – Ak m = 24, potom subpole CAIntMess, ktoré má dĺžku 32 bajtov, bude sa prenášať v dvoch rámcoch.)

G.1 Záhlavie predvoľby

Na prenesenie subpoľa CAIntMess v poli PrefixDataField sa musia správy rozdeliť do paketov. Bity 1 až 7 záhlavia predvoľby obsahujú informácie o identifikátore a pozícii paketu. Pomocou týchto bitov sa môžu v koncovom zariadení pôvodné správy znova usporiadať. Bit 0 sa prepína na indikáciu zmeny riadiaceho slova.

– Prvá návesť (FF) 1 bit;
– posledná návesť (LF) 1 bit;
– paket Id (PI) 2 bity;
– indikátor paketizácie (PP) 1 bit;
– index kontinuity (CI) 2 bity;
– prepínač riadiaceho slova (CWT) 1 bit.

Prvá návesť (FF), posledná návesť (LF)

Návesti sa používajú na identifikáciu jednotlivých paketov, ktoré tvoria túto postupnosť paketov:

FF	LF	Tento paket je:
0	0	prechodný paket
0	1	posledný paket správy
1	0	prvý paket správy
1	1	jediný paket správy

Paket ID (PId): Pole indikuje identifikátor paketu. Týmto spôsobom sa môžu realizovať až 4 logické transportné paralelné kanály, napríklad súrna správa v subpoli CAIntMess môže prerušiť a predbehnúť iné správy.

PId	Tento paket patrí:
00	logickému transportnému kanálu 0
01	logickému transportnému kanálu 1
10	logickému transportnému kanálu 2
11	logickému transportnému kanálu 3

Indikátor paketu s výplňou (PP): Bit indikuje, či sú použité všetky bajty v poli PrefixDataField. Ak napríklad posledný paket postupnosti potrebuje len n bajtov poľa (n < 256), potom prvý bajt poľa PrefixDataField obsahuje počet použitých bajtov. Jeho hodnota nezahŕňa celkový počet bajtov.

PId	Význam
00	Nevykonáva sa paketizácia: použité sú všetky dátové bajty poľa PrefixDataField
01	Paketizácia sa vykonáva: prvý bajt je kódovaný ako celé číslo bez znamienka, v poli PrefixDataField udáva počet nepoužitých bajtov, nepoužité bajty sú nastavené na 0x00

POZNÁMKA. – Keďže n je kódované ako osembitové celé číslo, n musí byť menšie ako 256. S n = 256 má pole SUBCAPrefix dĺžku 259 bajtov, čo zodpovedá rýchlosti viac ako 80 kbit/sekundu.

Index kontinuity(CI): Dvojbitové pole narastá o 1 modulo 4 s každým paketom s rovnakým identifikátorom paketu, čo umožňuje detegovať stratu paketov.

Prepínač riadiaceho slova (CWT): Bit nie je spojený s nasledujúcim poľom PrefixDataField, ale so skramblovaným rámcom, ktorý nasleduje za poľom SUBCAPrefix. Signalizuje aktuálne použité riadiace slovo a jeho prepínanie indikuje zmenu riadiaceho slova. CWT je synchronizačným parametrom CA (pozri prílohu E).

G.2 Dátové pole predvoľby

Dátové pole predvoľby prenáša subpole podmieneného prístupu k systému vnútorných správ (CAIntMess). Jeho ďalšie použitie, štruktúra a kódovanie sú špecifické v každom systéme CA a navzájom sa odlišujú.

Keď je v záhlaví predvoľby indikátor paketu s výplňou (PP) nastavený na 1, prvý bajt v poli PrefixDataField udáva počet použiteľných bajtov v poli PrefixDataField. Nepoužité bajty sú nastavené na 0x00.

Okrem subpoľa podmieneného prístupu k systému vnútorných správ (CAIntMess) sa tu môžu umiestniť tieto identifikátory:

ShortCASysId: Ako sa vysvetľuje v čl. 4.4 a 5.2.2, na realizáciu koncepcie so zdieľaným skramblerom každé subpole CAIntMess prenášané v poli PrefixDataField sa začína trojbitovým identifikátorom ShortCASysId.

Počítadlo rámcov: pozri prílohu E. Pomáha udržiavať v synchronizácii deskrambler koncového zariadenia.

Odpočet zmeny riadiaceho slova: pozri prílohu E. Indikuje počet zostávajúcich rámcov do objavenia sa zmeny riadiaceho slova.

Inicializačný modifikátor: pozri prílohu E.

Riadenie komunikácie CA: pozri prílohu E.

G.3 CRC

Šestnásťbitová cyklická kontrola redundancie sa počíta z poľa PrefixHeader a z poľa PrefixDataField. Je generovaná podľa procedúr definovaných v čl. 5.3.3.3 EN 300 401 [1].

História

História dokumentu		
V1.1.1	Január 2005	Publikácia
V1.2.1	Január 2006	Publikácia